Comptroller and Auditor General of India

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Notice Inviting Tender

Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

'One IA&AD One System' (OIOS) Project

Reference Number: 51-ISW/2019-One IAAD One System Project

Tender Data Sheet and Timelines

Tender Inviting Authority	Comptroller and Auditor General of India, New Delhi
Name of the Project Work	Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of 'One IA&AD One System' (OIOS) Project
Tender ID	2019_CAG_496493
Tender Reference No.	51-ISW/2019-One IAAD One System Project
The tender document issued to	This invitation for bids is open to all Indian firms who fulfil pre-qualification criteria as specified in Volume II of the RFP
Start Date for issue of the Tender document	As per CPP Portal https://eprocure.gov.in/eprocure/app
Last Date to submit NDA, Integrity Pact and receive the Tender Document by the shortlisted Bidders	As per CPP Portal https://eprocure.gov.in/eprocure/app
List of Tender documents (RFPs)	Volume I – Functional, Technical and Operational Requirements Volume II – Commercial and Bidding Terms Volume III – Master Services Agreement
The Contact Person	Sreeraj Ashok Deputy Director (IS) Office of the Comptroller and Auditor General of India 9, Deen Dayal Upadhyaya Marg, New Delhi-110124 Phone: 011-23235055

	oios@cag.gov.in
Address to send Pre-bid queries	Queries for clarifications on RFP document must reach through E-mail on or before the date of Pre-bid Conference
Last date to receive Pre-bid queries	As per CPP Portal https://eprocure.gov.in/eprocure/app
Place for Pre-bid meeting	iCISA, A-52, Institutional Area, Block A, Industrial Area, Sector 62, Noida, Uttar Pradesh 201301 0120-2400050/52
Date and time of Pre-bid meeting	As per CPP Portal https://eprocure.gov.in/eprocure/app
The starting of bid submission	As per CPP Portal https://eprocure.gov.in/eprocure/app
Last date and time for submission of bid	As per CPP Portal https://eprocure.gov.in/eprocure/app
Mode of submission of bids	Only Online Bids through CPP Portal at https://eprocure.gov.in/eprocure/app
The Fees	RFP Document can be downloaded free of cost from https://eprocure.gov.in/eprocure/app
Last date to receive EMD **(Physical Instrument)**	Friday 27th Sep 2019
Technical Bid opening	As per CPP Portal https://eprocure.gov.in/eprocure/app
Validity of the Proposal	180 days from the date of Bid Submission Closing

Commercial bid opening	Will be notified later
Nature of bid process	Open Tender

EMD and PBG Details

	EMD	PBG
EMD/PBG Amount	Rs 25,00,000/- (Rupees Twenty Five Lakhs only)	10% of total contract value of the contract
Mode of payment	Demand Draft OR Bankers Cheque OR Bank Guarantee	Bank Guarantee as per the format from any Commercial Bank.

General Instructions to Bidders

1. This RFP is not an offer by CAG but an invitation to receive proposals only from eligible bidders in respect of the above-mentioned project. The RFP does not commit CAG to enter into a binding agreement in respect of the project with any eligible bidder
2. The RFP document can be downloaded Free of Cost from the websites mentioned in the fact sheet
3. The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP documents. Failure to furnish all information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the bidder's risk and may result in rejection of the proposal and forfeiture of the bid security.
4. Submission of a bid in response to this invitation shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications.
5. Failure to furnish all information required by the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the Bidder's risk and may result in rejection of its Proposal.
6. Proposals must be direct, concise and complete. CAG will evaluate bidders proposal based on its clarity and directness of its response to the requirements of the project as outlaid in this RFP.
7. CAG's decision with regard to the selection of bidders through this RFP shall be final and

CAG reserves the right to reject any or all the bids without assigning any reason.

Annexure I. Format of Covering Letter of proposal in response to RFP Invitation

To:

<Location, Date>

<Name>

<Designation>

<Address>

<Phone Nos.>

<email id>

Subject: Submission of proposal in response to the RFP for Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of 'One IA&AD One System' (OIOS) Project.

Ref.: RFP No ....dated ....

Dear Sir,

Having examined the RFP document, we, the undersigned, herewith submit our proposal in response to your RFP No ....dated................... for RFP for Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of 'One IA&AD One System' (OIOS) Project.

a. We have read and understood the provisions of the RFP document and confirm that these are acceptable to us. We conform that only the terms and conditions in the RFP shall apply; we further declare that additional conditions, variations, deviations, if any, found in our bid shall be without any effect whatsoever.

b. We hereby declare that we satisfy all the eligibility criteria as specified in this RFP and agree to abide by all the terms and conditions specified therein.

c. We agree to abide by this bid, consisting of this letter, the detailed response to the RFP and all attachments, and validity of the bid shall be for a period of << enter bid validity period mentioned in the fact sheet>> days from the closing date fixed for submission of bids as stipulated in the RFP document.

d. The Earnest Money Deposit (EMD) of Rs 25,00,000/- (Rupees Twenty Five Lakhs only) submitted by us in the form of Demand Draft or Banker Cheque or Bank Guarantee may be forfeited under any of the circumstances as specified under sub-section on EMD of this RFP.

e. We hereby declare that we are not involved in any litigation that may have an impact of affecting or compromising the delivery of services as required under this assignment and we are not under a declaration of ineligibility for corrupt or fraudulent practices.

f. We confirm that we have not been banned / blacklisted by the Central Government/PSU any other Central Government institutions in India for any reason as on the last date of submission of the Bid or convicted of economic offence in India for any reason as on the last date of submission of the Bid.

g. We hereby declare that all the information and statements made in this bid are true and accept that any misrepresentation/wrong information contained in it or /suppression of material or relevant facts/figures may lead to our disqualification

h. We understand that you are not bound to shortlist / accept any proposal you receive.

Our correspondence details with regards to this bid are:

S. No.	Information	Details
1.	Name of responding firm:	
2.	Address of responding firm:	
3.	Name, Designation and Address of the	
	contact person to whom all references	
	shall be made regarding this RFP:	
4.	Telephone no. of contact person:	
5.	Mobile no. of contact person:	
6.	Fax no. of contact person:	

7.	E-mail address of contact person:	
8.	Website URL of the responding firm	

We hereby declare that our bid submitted in response to this RFP is made in good faith and the information contained is true and correct to the best of our knowledge and belief.

Yours faithfully,

[FIRM'S NAME]

Authorized Signature [In full and initials]

Date:

Place

Name and Title of Signatory:

Address of Firm:

Seal of the Firm:

Annexure II. Bank Guarantee Format for EMD/ Bid Security

To,

<Name>

<Designation

<Address>

<Phone Nos.>

<email id>

Whereas <<Name of the Bidder>> (hereinafter called 'the Bidder') has submitted the bid for Submission of RFP # <<RFP Number>> dated <<Date>> for <<Implementation of One IAAD and One System>> (hereinafter called "the Bid") to IA&AD

Know all Men by these presents that we << >> having our office at <<Address>> (hereinafter called "the Bank") are bound unto the Comptroller and Auditor General of India, (hereinafter called "the Purchaser") in the sum of Rs. <<Amount in figures>> (Rupees <<Amount in words>> only) for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this <<Date>>

The conditions of this obligation are listed in Section 7.3.3 of Vol II of the RFP:

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or more of the conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to <<insert date>> and including <<extra time over and above mandated in the RFP>> from the last date of submission and any demand in respect thereof should reach the Bank not later than the above date.

NOTHWITHSTANDING ANYTHING CONTAINED HEREIN:

I. Our liability under this Bank Guarantee shall not exceed Rs. <<Amount in figures>> (Rupees <<Amount in words>> only)

II. This Bank Guarantee shall be valid upto <<insert date>>)

III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before <<insert date>>) failing which our liability under the guarantee will automatically cease.

IV. We also undertake not to revoke this guarantee during this period except with the previous consent of the Purchaser in writing and we further agree that our liability under the EMD / Bid Security shall not be discharged by any variation in the term of the said RFP and we shall be deemed to have agreed to any such variation.

V. No interest shall be payable by the Purchaser to the bidder on the guarantee for the period of its currency.

(Authorized Signatory of the Bank) Seal:

Date:

Annexure III. Performance Bank Guarantee Format

PERFORMANCE SECURITY:

To: <Location, Date>

<Name>

<Designation>

<Address>

<Phone Nos.>

<email id>

Whereas, <<name of the supplier and address>> (hereinafter called "the Bidder") has undertaken, in pursuance of contract no. <Insert Contract No.> dated. <Date> to provide Implementation services for Implementation of One IAAD and One System to Comptroller and Auditor General if India (hereinafter called "the beneficiary")

And whereas it has been stipulated by in the said contract that the Bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract;

And whereas we, <Name of Bank> a banking company incorporated and having its head /registered office at <Address of Registered Office> and having one of its office at <Address of Local Office> have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of Rs.<Insert Value> (Rupees <Insert Value in Words> only) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of Rs. <Insert Value> (Rupees <Insert Value in Words> only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the Bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you and the Bidder shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

This Guarantee shall be valid until <<Insert Date>>)

Notwithstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed Rs. <Insert Value> (Rupees <Insert Value in Words> only).

II. This bank guarantee shall be valid up to <Insert Expiry Date>)

It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before <Insert Expiry Date>) failing which our liability under the guarantee will automatically cease.

Annexure IV. Integrity Pact

PRE-CONTRACT INTEGRITY PACT

General

1. Whereas CA&G, hereinafter referred to as Purchaser and the first party, proposes to implement Project "Implementation of One IAAD One System", hereinafter referred to as Project, and M/s ___________________________________, represented by, ________________________ << Designation>> (which term, unless expressly indicated by the contract, shall be deemed to include its successors and its assignees), hereinafter referred to as the Bidder/Seller and the second party, is willing to offer/has offered IA&AD

2. Whereas the Bidder is a private company/public company/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the Purchaser is IA&AD performing its duty on behalf of GoI.

Objectives

3. Now, therefore, the Purchaser and the Bidder agree to enter into this pre-contract agreement, hereinafter referred to as Integrity Pact, to avoid all forms of corruption by following a system that is fair, transparent and free from any influence / unprejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:

   a. Enabling the Purchaser to implement the desired "Implementation of One IAAD One System" a competitive price in conformity with the defined specifications of the Services by avoiding the high cost and the distortionary impact of corruption on public procurement, and

   b. Enabling bidders to abstain from bribing or any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also refrain from bribing and other corrupt practices and the Purchaser will commit to prevent corruption, in any form, by their officials by following transparent procedures

Commitments of the Buyer

4. The Purchaser commits itself to the following:

   a. The Purchaser undertakes that no official of the Purchaser, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the Bidder, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the Contract.

b. The Purchaser will, during the pre-contract stage, treat all Bidders alike, and will provide to all Bidders the same information and will not provide any such information to any particular Bidder which could afford an advantage to that particular Bidder in comparison to other Bidders.

c. All the officials of the Purchaser will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

5. In case of any such preceding misconduct on the part of such official(s) is reported by the Bidder to the Purchaser with full and verifiable facts and the same is prima facie found to be correct by the Buyer, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the Purchaser and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the Buyer the proceedings under the contract would not be stalled.

Commitments of Bidders

6. The Bidder commits himself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of his bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commits himself to the following:

   a. The Bidder will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Purchaser, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the Contract.

   b. The Bidder further undertakes that he has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Purchaser or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the Contract or forbearing to show favour or dis-favor to any person in relation to the Contract or any other Contract with the Government.

c. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

d. The Bidder will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

e. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

f. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

g. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

h. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

i. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

j. The Bidder shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

7. Previous Transgression

a. The Bidder declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify bidder's exclusion from the tender process.

b. If the Bidder makes incorrect statement on this subject, Bidder can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

8. Bank Guarantee

In the case of the successful bidder, a clause would also be incorporated in the Article pertaining to Performance Bank Guarantee in the Purchase Contract that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bank Guarantee in case of a decision by the Buyer to forfeit the same without assigning any reason for imposing sanction for violation of this pact.

9. Company Code of Conduct

Bidders are also advised to have a company code of conduct (clearly rejecting the use of bribes and other unethical behaviour) and a compliance program for the implementation of the code of conduct throughout the company.

10. Sanctions for Violation

a. Any breach of the aforesaid provisions by the Bidder or any one employed by him or acting on his behalf (whether with or without the knowledge of the Bidder) or the commission of any offence by the Bidder or any one employed by him or acting on his behalf, as defined in Chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act 1988 or any other act enacted for the prevention of corruption shall entitle the Purchaser to take all or any one of the following actions, wherever required:

   i. To immediately call off the pre-contract negotiations without assigning any reason or giving any compensation to the Bidder. However, the proceedings with the other Bidder(s) would continue.

   ii. To immediately cancel the contract, if already signed, without giving any compensation to the Bidder.

iii. The Performance Bank Guarantee / Other Guarantee shall stand forfeited either fully or partially, as decided by the Buyer and the Buyer shall not be required to assign any reason therefore

~~iv.~~ To recover all sums already paid by the Purchaser, in case of an Indian Bidder with interest thereon at 2% higher than the prevailing RBI Bank Rate.

v. To encash the advance bank guarantee and Performance-Bank Guarantee if furnished by the Bidder, in order to recover the payments, already made by the Buyer, along with interest.

vi. To cancel all or any other Contracts with the Bidder.

vii. To debar the Bidder from entering into any bid from the Government for India for a minimum period of five years, which may be further extended at the discretion of the Purchaser.

viii. To recover all sums paid in violation of this Pact by Bidder to any middleman or agent or broker with a view to securing the contract.

ix. If the Bidder or any employee of the Bidder or any person acting on behalf of the Bidder, either directly or indirectly, is closely related to any of the officers of the Purchaser, or alternatively, if any close relative of an officer of the Purchaser has financial interest/stake in the Bidder's firm, the same shall be disclosed by the Bidder at the time of filling the tender. Any failure to disclose the interest involved shall entitle the Buyer to rescind the contract without payment of any compensation to the Bidder.

x. The term 'close relative' for this purpose would mean spouse whether residing with the Government servant or not, but not include a spouse separated from the Government servant by a decree or order of a competent court; son or daughter or step son or step daughter and wholly dependent upon Government servant, but does not include a child or step child who is no longer in any way dependent upon the Government servant or of whose custody the Government servant has been deprived of by or under any law; any other person related, whether by blood or marriage, to the Government servant or to the Government servant's wife or husband and wholly dependent upon Government servant.

xi. The Bidder shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the Purchaser, and if he does so, the Purchaser shall be entitled forthwith to rescind the contract and all other contracts with the Bidder. The Bidder shall be liable to pay compensation for any loss or damage to the Buyer resulting from such rescission and the Buyer shall be entitled to deduct the amount so payable from the money(s) due to the Bidder.

xii. In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the Buyer with the Bidder, the same shall not be opened.

b. The decision of the Purchaser to the effect that a breach of the provisions of this Integrity Pact has been committed by the Bidder shall be final and binding on the Bidder, however, the Bidder can approach the monitor(s) appointed for the purposes of this Pact.

11. Fall Clause

a. The Bidder undertakes that he has not supplied/is not supplying the similar systems or subsystems at a price lower than that offered in the present bid in last 2 Years (from the date of bid submission) in respect of any other of any other project of similar size Ministry/Department of the Government of India and if it is found at any stage that the similar system of sub-system was supplied by the Bidder to any other Ministry / Department of the Government of India at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the Bidder to the Purchaser, if the contract has already been concluded.

b. The Bidder shall accord the most favoured customer treatment to the buyer in respect of all matters pertaining to the present case

12. IA&AD **Examination of Book of Records**

In case of any allegation of violation of any provisions of this Integrity Pact or payment of commission, the Purchaser or its agencies shall be entitled to examine the Books of Accounts of the Bidder and the Bidder shall provide necessary information of the relevant financial documents in English and shall extend all possible help for the purpose of such examination.

13. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the Purchaser i.e. New Delhi.

14. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

15. Validity

The validity of this Integrity Pact shall be from date of its signing and extend up to 5 years or the complete execution of the contract to the satisfaction of both the Purchaser and the Bidder/Seller, whichever is later.

Should one or several provisions of this pact turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

The Parties hereby sign this Integrity Pact at __________ on _____________.

IA&AD

PURCHASER BIDDER

Witness

1. 1.

2. 2.

Annexure V. Bid Clarification Format

S. No.	RFP document reference(s) (RFP Vol , Section & page number)	Content of RFP requiring clarification(s)	Observation/ Suggestion	Type of observation (Compliance issue, suggestion)	Justification

Comptroller and Auditor General of India

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Request for Proposal

`Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

'One IA&AD One System' (OIOS) Project

VOLUME - I

Reference Number: 51-ISW/2019-'One IA&AD One System' Project

Page Intentionally Left Blank

Disclaimer

The information contained in this Request for Proposal document (“RFP”) or subsequently provided to Bidders, whether verbally or in documentary or any other form by or on behalf of the Comptroller & Auditor General of India (C&AG/ IA&AD), or any of its employees or advisors, is provided to Bidders on the Terms and Conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is neither an offer nor an invitation by IA&AD to the prospective Bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in the formulation of their Proposals pursuant to this RFP.

This RFP may not be appropriate for all companies, and it is not possible for IA&AD, its employees or advisers to consider the objectives, technical expertise and particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP, may not be complete, accurate, adequate or correct. Each bidder should therefore conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments and information contained in this RFP and obtain independent advice from appropriate sources.

Information provided in this RFP to the Bidders is on a wide range of matters, some of which depends upon interpretation of facts. The information given is not an exhaustive account of requirements and should not be regarded as a complete or authoritative statement of facts. The specifications laid out in this RFP are indicated as the minimum requirements whereas the bidders are expected to focus on the objectives of the project and formulate their solution offerings in a manner that enables achieving those objectives in letter as well as spirit.

IA&AD accepts no responsibility for the accuracy or otherwise for any interpretation or opinion expressed herein. IA&AD, its employees and advisors make no representation or warranty and shall have no liability to any person including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, reliability or completeness of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process.

Page Intentionally Left Blank

`

1. Table of Contents

`

`

`

Glossary of Acronyms

Acronym	Full text
AD	Active Directory
ADM	Audit Design Matrix
AMC	Annual Maintenance Contract
API	Application Program Interface
APM	Application Performance Monitoring
APT	Advanced Persistent Threat
BI	Business Intelligence
BCP	Business Continuity Planning
BPM	Business Process Management
C&AG	Comptroller and Auditor General of India
CERT-In	Indian Computer Emergency Response Team
CIN	Corporate Identification Number
CMMI	Capability Maturity Model Integration
CPU	Central Processing Unit
COTS	Commercial Off-The-Shelf product
CPP	Central Public Procurement
DC	Data Center
DMS	Document Management System
DMZ	Demilitarized zone
DR	Disaster recovery
DRC	Disaster Recovery Centre
DW	Data Warehouse
EMD	Earnest Money Deposito
EMS	Event Monitoring Service

Acronym	Full text
FAO	Field Audit Office
GFR	General Financial Rules
GIS	Geographical Information System
GOI	Government of India
GST	Goods & Services Tax
GUI	Graphical User Interface
HQ	Headquarters
HR	Human Resources
HSM	Hardware Security Module
IA&AD	Indian Audit and Accounts Department; often used interchangeably with C&AG (Comptroller and Auditor General of India)
ICISA	International Centre for Information Systems and Audit
ICT	Information & Communication Technology
IEC	International Electro-technical Commission
IFMS	Integrated Financial Management System
INR	Indian Rupee
IP	Internet Protocol
IPMP	Integrated Project Management Plan
IR	Inspection Report
IS	Information System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITA	Internal Test Audit
IW	Inspection Wing

`

Acronym	Full text
KD	Key Document
KMS	Knowledge Management System
KPI	Key Performance Indicator
LAN	Local Area Network
LB	Local Bodies
LC	Legislative Committee
LLP	Limited Liability Partnership
LOI	Letter of Intent
LTO	Linear Tape Open
MeitY	Ministry of Electronics & Information Technology
MIS	Management Information System
MPLS	Multi-Protocol Label Switching
MSA	Master Services Agreement
MZ	Militarized Zone
NAC	Network Access Control
NCR	National Capital Region
NICNET	National Informatics Centre Network
NLDC	Near Line Data Center
NLSAS	Near Line SAS
O&M	Operations and Maintenance
OEM	Original Equipment Manufacturer
OIOS	One IA&AD One System
OS	Operating System
OSC	OIOS Steering Committee
OWASP	Open Web Application Security Project

`

Acronym	Full text
PAC	Public Accounts Committee
PAN	Permanent Account Number
PAO	Pay and Accounts Officer
PBG	Performance Bank Guarantee
PC	Personal Computer
PDC	Primary Data Centre
PECMC	Project Execution and Change Management Committee
PFMS	Public Financial Management System
PR	Peer Review
QA/QC	Quality Assurance/ Quality Control
QCBS	Quality cum Cost Based Selection
RAM	Random Access Memory
RBP	Record Based Permission
RDBMS	Relational Database Management System
RFP	Request For Proposal
ROC	Registrar of Companies
RPO	Recovery Point Objective
RTI	Right To Information Act
RTO	Recovery Time Objective
SAI	Supreme Audit Institution
SAN	Storage Area Network
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SI	System Integrator
SIEM	Security information and event management

`

Acronym	Full text
SLA	Service Level Agreement
SQL	Structure Querying Language
SSD	Solid State Device
STQC	Standardisation Testing and Quality Certification
TGS	Technical Guidance and Support
TK	Toolkit
UAT	User Acceptance Testing
UTF	Unicode Transformation Format
VAPT	Vulnerability Assessment Penetration Testing
VLAN	Virtual Local Area Network
VLC	Voucher Level Computerization
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall

2. Request for Proposal

Tenders are invited from eligible, reputed, qualified Information Technology (IT) firms with sound technical and financial capabilities for design, development, implementation and maintenance of an enterprise-wide end to end IT solution as detailed out in the scope of work of this RFP Volume 1. This invitation to bid is open to all bidders meeting the minimum eligibility criteria as mentioned in RFP Vol 2 document.

3. Structure of the RFP

The structure of this RFP is as follows.

Volume I: Functional, Technical, Operational and Other Requirements

Volume I of the RFP intends to bring out all the details with respect to scope of work, project implementation, timelines, solution and other requirements that IA&AD deems necessary to share with the potential bidders. The information set out in this volume has been broadly categorized as Functional, Technical and Operational requirements covering multiple aspects of the requirements.

Volume II: Commercial and Bidding Terms

Volume II of the RFP intends to detail out all that may be needed by the potential bidders to understand the commercial terms and bidding process details.

Volume III: Master Service Agreement

Volume III of the RFP is essentially devoted to explain the contractual terms that IA&AD wishes to specify at this stage. It basically consists of a draft of Master Services Agreement (MSA) that needs to be signed between the IA&AD and the Selected Bidder. This MSA includes a separate schedule on Service Level Agreement (SLA).

The bidders are expected to examine all instructions, forms, terms, Project requirements and other information in the RFP documents. Failure to furnish all information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the Bidder's risk and may result in rejection of the proposal.

This document is Volume 1.

`

4. Background information

The background information regarding the Department, project and the vision of the project is detailed below.

4.1. About IA&AD

The Comptroller and Auditor General (C&AG) of India is a Constitutional authority, who discharges his functions through the Indian Audit and Accounts Department (IA&AD). It is the duty of the C&AG to audit the receipts and expenditure of the Union and each State and Union Territory Government, and such other functions as prescribed by or under laws made by Parliament. The Audit Reports of the Comptroller and Auditor General are placed before Parliament or the Legislature of the State/ Union Territory, as the case may be. More information about the C&AG and IA&AD is available at https://cag.gov.in/ in particular, the Performance Report for 2017-18 at https://cag.gov.in/sites/default/files/performance_activity_report/PA_2018_1.pdf.

4.2. Project Background

The IA&AD Department is headquartered at New Delhi and has several categories of Field Offices (FOs), viz. Field Audit Offices (FAOs), Accounts & Entitlement (A&E) offices and training institutes. There are 94 field audit offices spread across the country and some field audit offices also have branch offices[1] at various locations. These field audit offices are responsible for discharging the functions relating to audit of receipts and expenditure of the Union, State, and Union Territory Governments and other auditable entities. Some of the wings in the headquarters of IA&AD (C&AG HQ) are responsible for providing Quality Assurance/ Quality Control for activities of field audit offices under their jurisdiction. The field audit offices spread across the country fall under different categories and sub-categories. These are referred to '**audit streams**' (see illustration below). Each field audit office engages in three types of audit, 'Financial audit', 'Compliance audit' and 'Performance audit' or combinations thereof. Though the fundamental core audit processes remain the same in the field audit offices, the audit

[1] There are approximately 62 branch offices. This brings the total number of user offices (field audit offices and branch offices) to 156 approximately.

streams and types of audit have given rise to various flavours of audit processes in IA&AD over the 150 years.

Audit streams in Indian Audit and Accounts Department

1. Audit Offices for the Union Government
    - 1.1. Civil Audit
        - 1.1.1.Central expenditure audit
        - 1.1.2.Central revenue audit
    - 1.2. Defence Audit
    - 1.3. Posts & Telecommunications Audit
    - 1.4. Railways Audit
    - 1.5. Commercial Audit
2. Audit Offices for State Governments
    - 2.1. State Civil audit
    - 2.2. State receipt audit
    - 2.3. State commercial audit
    - 2.4. Technical Guidance and Support of PRIs and ULBs
3. Overseas and External Audit Offices

The purpose of the 'One IA&AD One system' (OIOS) project is to create an IT based platform, which will create a single source of truth regarding audit activities of IA&AD. IA&AD has seen several IT applications that catered to the needs of one or more offices/ audit streams in this regard. OIOS will bring together the best practices of the various IT applications into one single enterprise-wide end-to-end IT application. This IT application will be designed in such a way that it can be configured and used by any audit office (**any audit stream and any type of audit**) in the IA&AD, and also be configurable to implement future changes in audit processes, products etc.

4.3. OIOS Vision

Vision Statement

To make our audit more effective by empowering IA&AD officials from the audit team upwards, and to make our audit processes more efficient and *effective through a state of the art end-to-end IT solution, with seamless integration and process workflow.*

The current scenario of information availability within the IA&AD with regard to audit[2] is as follows:

- Information is stored in a **heterogeneous and distributed manner** – in paper-based files (accessible only through file number and title, or through personal knowledge), in electronic files (but with haphazard naming and versions, and stored on personal desktops/ removable drives, or in some cases shared folders on LANs) and in some cases in localized, in-house IT systems (but without a common data dictionary).
- The **quality of data (paper based/ digital) is variable** – In the absence of automated control mechanisms, there are significant risks of incompleteness of data, inaccuracies, version inconsistencies etc. This is accentuated by the fact that even the in-house IT systems are largely based on post-facto data entry.
- There are no mechanisms for **systematic sharing of data** – whether it is from one audit assignment to other, similar audit assignments in the future, or between audit offices (field/ Headquarters). Each individual audit assignment is an end in itself, and there are no real mechanisms for using past data (or data from other similar instances). Any such sharing or exchange that takes place is person-dependent (or very occasionally, manual process dependent)
- Although our audit processes are governed by centralized Auditing Standards, Guidelines and Manuals, these have **tended to, over time[3], vary and deviate** across audit streams and even across audit offices within the same audit streams. Many of these variations are consciously done due to differences in functional needs, but some are not (and this is accentuated by the lack of automation).
- There are **no significant automated/ electronic MISs** covering audit activities, whether within the Field Audit Offices or from the FAOs to Headquarters. Within Field Audit Offices, control is to be exercised through submission of manual registers and manually compiled “returns” to be submitted for review according to a prescribed hierarchy and frequency of submission. Similarly, Field Audit Offices submit a variety of “returns” to Headquarters Office.

[2] This section does not apply to other field offices of IA&AD – viz. A&E Offices and Training Institutes.

[3] The Department dates back more than 150 years, and some of our Field Audit Offices are close to a century old.

Our **high-level vision for OIOS** in IA&AD is as follows:

- OIOS will be an end-to-end enterprise-wide, integrated IT system for all audit activities in IA&AD, covering all Field Audit Offices and the Headquarters Office. It will be the primary system of record (single source of truth) for the entire chain of audit activities (from the maintenance of the auditee universe through audit execution, to QA/QC and finalization of audit products of different types and their follow-up), and will cover all types of audit. It will be a workflow-based IT system, and not based on post-facto data entry.
- OIOS will have a common core structure and minimum required mandatory functionality (which will ensure consistent, reliable data in a uniform format across all Audit Offices). At the same time, it will provide for "**configurable**" functionality, which can be configured audit stream/ audit office/ wing-wise, and can also be configured/ re-configured over time. It will also have an MIS with configurable dashboards and drill-down, dispensing with paper-based registers and returns.
- OIOS is not just an audit process management system. An equally important component of OIOS is to empower the auditor in various ways – (a) through a KMS with both audit guidance and auditee information in different formats, (b) the ability to search through and mine data within OIOS to refine our audit approach and processes (c) the ability to electronically link and reference (and re-use) supporting documentation and other evidence (e.g. geo-tagged, time-date stamped formats) (d) IT-enabled audit toolkits to facilitate implementation of Audit Design Matrices in individual audit assignments.
- OIOS will be a web-enabled solution with support for multiple languages, accessible in a platform-independent manner. Limited offline functionality, as also a mobile app, will be available as a back-up to the field audit teams. At the same time, rigorous information security controls (for maintaining confidentiality, integrity, availability and non-repudiability) will be implemented, and access to data will be controlled on a need-to-know basis.

5. Overarching strategy for product (OIOS IT solution) delivery

The overarching requirement for product delivery is to employ agile development methodology to develop the OIOS IT solution. There are many different software development models which employ agile development methodology. For the purposes of this RFP, we have adopted concepts and language used in the Scrum methodology. However, the bidder may suggest an alternate agile flavour.

`

IA&AD is also not prescribing a specific DevOps Toolchain that will aid in the development, delivery and management of software; the specific Toolchain may be suggested by the bidder.

5.1. Adapting Agile for OIOS project (A hybrid approach)

The OIOS project aims at creating a single Enterprise wide IT platform for all audit activities of IA&AD. The OIOS IT solution should capture the common core audit processes and allow for "configuration" of the IT solution that is required by the different flavors of audit. In order to achieve this, instead of a standard agile approach, a hybrid agile approach is proposed. This adaptation is required because of the implementation strategy and the modular approach that is needed for successful implementation of the project. The same is explained in detail in this section.

5.1.1. Implementation strategy (Three stage)

The OIOS IT solution is proposed to be implemented in three stages in the IA&AD. Two representative groups of field audit offices have been selected for the purpose of implementation of OIOS project.

- The first group is a set of five to six (indicative) offices (geographically distributed), referred as '**pilot offices**' (**<u>Stage 1</u>**). The implementation in these pilot offices will assist in validating the design and development of core audit processes in the OIOS IT solution.
- The second group is a set of additional 25 to 26 (indicative) offices (geographically distributed), referred as '**nodal offices**[4]' (**<u>Stage 2</u>**) which is the representative sample of the flavors of audit. The implementation in these offices would assist in validating the ability of OIOS IT solution to be configured to suit the needs of the field audit offices.
- After both the validations, the OIOS IT solution would be implemented in the remaining field audit offices for an '**All-India**' implementation (**<u>Stage 3</u>**).

While the roll out in the pilot offices and nodal offices (Stages 1 and 2) are considered as part of 'development' and 'acceptance', the third stage is considered as 'roll-out' (i.e. no additional development from the SI should be required[5]).

[4] The total number of nodal offices is 31, out of which 5 to 6 will be covered as a subset under 'pilot offices'

[5] Any additional development required from the SI will be considered as "change management"

`

5.1.2. Modular approach

The business process of the IA&AD has been divided into modules and sub-modules of “business value”. This modularization does **NOT** reflect the modularization of OIOS IT solution. However, it is preferred that delivery of the IT solution or implementation of the IT solution may be made by bundling these business modules / sub-modules to offer “business value” to IA&AD. These bundles are broadly equivalent to ‘releases’ in agile methodology. Thus, the three-stage implementation strategy would be taken up for every release.

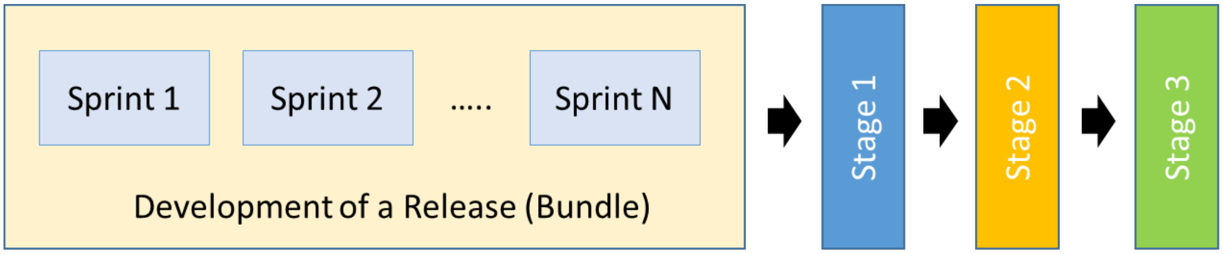
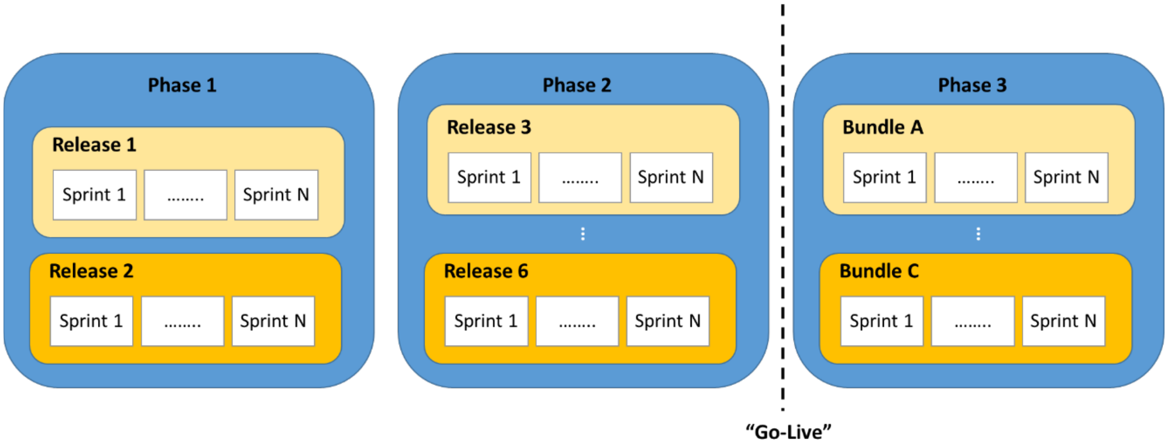


Figure 1: Three-staged implementation strategy for a release/bundle

5.1.3. Phasing of the OIOS IT solution

These bundles/ releases are proposed to be rolled-out in three phases. For the purpose of the RFP, the “Go-Live” is defined at the completion of Phase 2. The additional criteria for acceptance of “Go-Live” is detailed in **Section 23 : Definition of “Go Live”** in this document. The first phase is envisaged to have two releases (Release 1 and 2); the second phase with four releases (Release 3 through Release 6); the third phase with three bundles (loosely grouped sub-modules), Bundles A through C.



`

Figure 2: Phasing of the releases / bundles in OIOS project

5.1.4. Acceptance of development in OIOS's hybrid agile methodology

The three-stage implementation, the modular approach and the phasing, then means that there will be multi-stage client acceptance during the agile development.

The criteria for acceptance of a **user story** would be defined by the product owner and would include the following.

- Scope of tests to be conducted and passed (e.g. user acceptance tests and non-functional tests);
- Code review and compliance to coding standards; and
- Any necessary documentation has been completed.

The multi-stage acceptance consists of the following.

a) Sprint acceptance (Stage 0)

b) Release acceptance (Stage 1 and Stage 2)

c) Phase acceptance (Phase 1 and Phase 2)

Sprint acceptance - Stage 0 (Verification of core functionality): The product owner would provide '**Stage 0 acceptance**' based on review conducted by his core team. This acceptance testing would be done by the core team, after the sprint demo by SI, as part of sprint review. SI shall undertake the suggested corrective action and host the revised release and notify the product owner to once again validate the design at Stage 0.

Release acceptance - Stage 1 (Validation of core functionality): The product owner would provide '**Stage 1 acceptance**' based on review of core functionality by pilot offices and feedback provided by these offices to the product owner. This will be taken up in alignment with a release. SI shall undertake the suggested corrective action and host the revised release and notify the product owner to once again validate the design at Stage 1.

Release acceptance - Stage 2 (Verification & validation of configurability): The product owner would provide '**Stage 2 acceptance**' based on review of configurability by the nodal offices and feedback provided by these offices to the product owner. This will be taken up in alignment with a release. SI shall undertake the suggested corrective action and host the revised release and notify product owner to once again validate the design at Stage 2.

`

The multi-stage acceptance of sprint and a release is illustrated below.

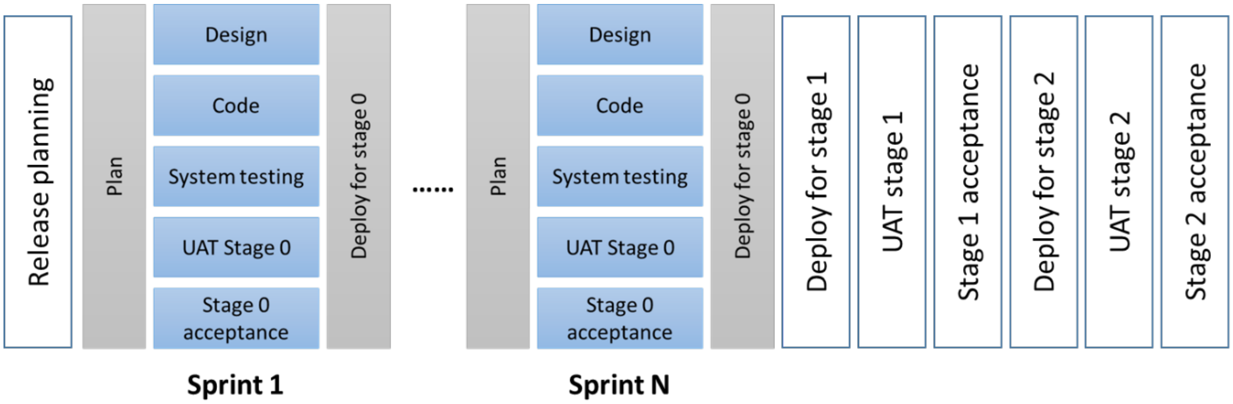


Figure 3: Sprint and release acceptance

Phase 1 acceptance: The product owner would provide 'Phase 1 acceptance' based on review of the functionalities of releases in phase 1, in an integrated manner, by his core team. This will be taken up in alignment with completion of phase 1. SI shall undertake the suggested corrective action and host the revised release and notify the product owner to once again validate the design at Phase 1. ***References to "Phase 1 Go-Live" anywhere in the RFP (i.e. Partial Go-Live) should be treated as completion of Phase 1 acceptance.***

Phase 2 acceptance: The product owner would provide 'Phase 2 acceptance' based on review of the functionalities of releases in phase 2, in an integrated manner, by his core team. This will be taken up in alignment with completion of phase 2. SI shall undertake the suggested corrective action and host the revised release and notify the product owner to once again validate the design at Phase 2.

Go-Live: After completion of phase 2 acceptance, the "Go-Live" acceptance would be provided by the product owner based on criteria detailed in **Section 23 : Definition of "Go Live"** in this document.

This multi-stage acceptance of the phase is illustrated below.

`

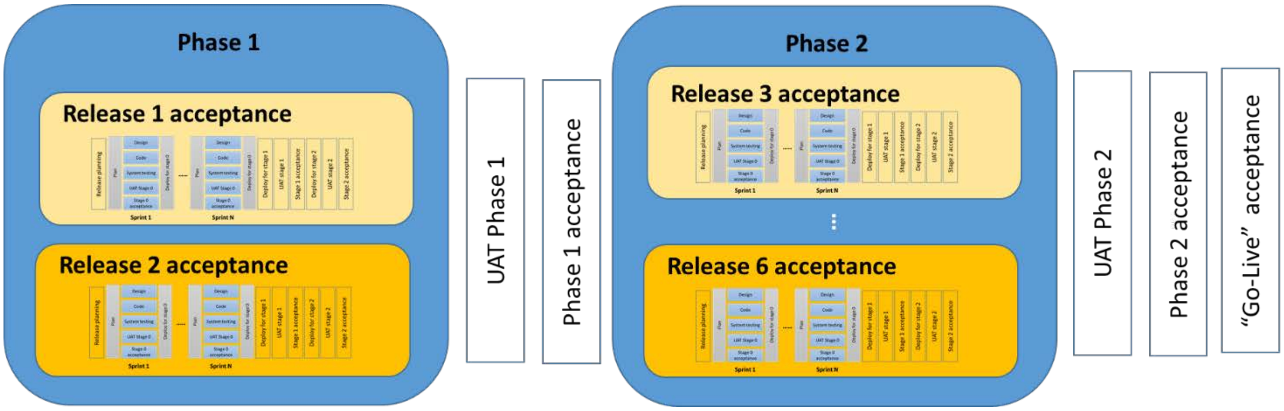


Figure 4: Phase-wise and final "Go-Live" acceptance

Technical Response from the Bidder in Technical Format 10 and 10A: The Bidder in the Technical response should propose a detailed Software Engineering approach for successfully completing OIOS Application for both phases 1 and 2 in **Technical Bid Format 10 with clear and precise reference to the Business Modules/ sub-modules of the said phases.**

The Bidder in the Technical response should propose Software Engineering approach for successfully developing OIOS Application Phase 3 requirements in **Technical Bid Format 10 B.**

`

6. Project Governance Structure

The OIOS project would require an institutional mechanism for effective supervision and appropriate project control. The high-level Project Governance Structure proposed to be employed for OIOS is depicted below. Since the software application development for OIOS is based on Agile methodology, this is appropriately reflected in the Project Governance Structure[6].

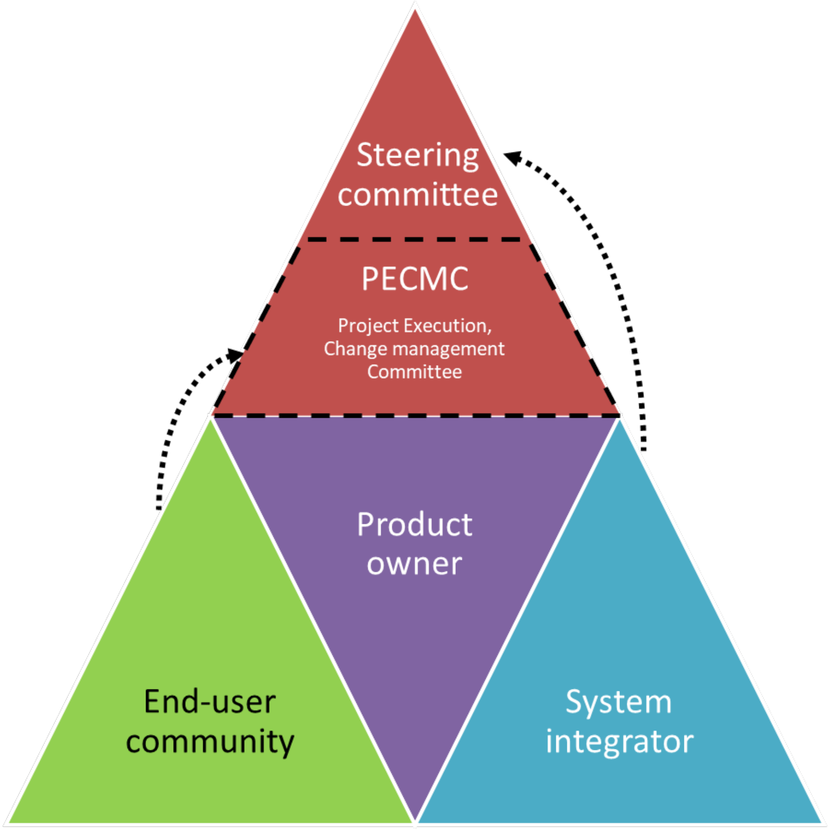


Figure 5: Project Governance Structure

A summary of the key functions and roles for different components of the OIOS Project Governance Structure is given below. The roles and responsibilities are elaborated in **Section 7 : Key stake holders, roles and responsibilities** in this document.

[6] For the purpose of laying down requirements, IA&AD has used the structure and terminology used in the Agile-Scrum methodology. However, the bidder may propose an alternate Agile flavour.

End-user community: The end-user community includes include internal users such as, officials of field audit offices, C&AG HQ and other relevant offices within IA&AD. They also include external users such as auditable entities and / or other agencies who may interact with the OIOS IT solution.

Product owner: The product owner is the key representative of IA&AD who is responsible for communicating the vision, objectives and the requirements for the project to the System Integrator (SI). The product owner is responsible for defining the deliverables of SI, determining the criteria for acceptance of deliverables made by the SI. He/ she is the sole-authority for signing-off of deliverables of SI after evaluating whether the deliverable meets the acceptance criteria. The product owner is also responsible for reporting project status to the project steering committee. The team of the product owner would consist of officials of IA&AD and other relevant specialists (internal and external). The team will be responsible for coordinating efforts of the end-user community and other agencies involved in OIOS project design, development, testing and implementation.

Project Execution and Change Management Committee (PECMC): This committee would consist of the product owner and other officials representing stakeholders across IA&AD. The committee would aid in building organisational synergy in IA&AD, that is essential for the change management process during implementation and roll-out of the OIOS IT solution. The core team of the product owner would need to work in tandem with the PECMC for smooth execution of the OIOS project.

Steering Committee: This committee would consist of senior officials of IA&AD. It would provide the required level of advocacy for the OIOS project and also set directions which are acceptable to all stakeholders. The role of this steering committee would be to provide strategic direction to the development and implementation of this project.

System integrator: The SI is responsible for design, development, implementation, operation and maintenance of the OIOS IT solution. The SI is responsible for timely delivery of identified deliverables with adequate quality, satisfying the criteria of the product owner. The SI may also be required to participate in the meetings with project steering committee, as and when required and address key issues raised by the product owner and project steering committee. The term 'System Integrator' includes, besides the SI, service provider of hosting services in Tier-3 co-located DC/DR and any other sub-contractor and outsourced resource(s) employed by SI.

`

The scope of work for the OIOS project along with the required parallel tracks are detailed in '**Section 7: in this document.**

The roles and responsibilities (including track-wise responsibilities) of stakeholders of the OIOS project are elaborated in **'Section 8.8 : OIOS Track-wise Responsibility Matrix**' in this document.

6.1. Project Governance Reporting Charter

S No	Committee/Team	Frequency of Meetings
1.	Steering Committee	Monthly for phase 1 & as and when required.
2.	Project Execution and Change Management Committee	Twice a month for phase 1 & as and when required.
3.	Product owner and System Integrator	Weekly for phase 1 & as and when required.

7. Key stake holders, roles and responsibilities

The Governance structure of the project consists of

1. OIOS Steering Committee (OSC)
2. Project Execution and Change Management Committee (PECMC)
3. Product owner (and his team)
4. System Integrator (SI)

The responsibilities, amongst others, are broadly described in the subsequent sections.

7.1. OIOS steering committee

The IA&AD will have the responsibility for overall policy directives, guidance and coordination for all project activities related to OIOS System. At a strategic level, this responsibility will be vested in the OIOS Steering Committee (OSC). The OSC will be responsible for:

- Guiding the work of the product owner and his team.
- Reviewing implementation progress periodically.
- Considering recommendations put forward by product owner.
- Strategic control over the OIOS project.
- Identification of IA&AD offices for phase wise Rollout of OIOS System.

7.2. Product owner and team (in tandem with PECMC)

The Product Owner will be an officer from IA&AD who is the key representative of IA&AD who will communicating the vision, objectives and the requirements for the project to the System Integrator (SI). The product owner is supported by a core team consisting of officials of IA&AD and specialists (internal and external). The product owner has the authority to delegate some of the functions detailed below to one or more members of the core team. Further, the product owner and the PECMC would need to work in tandem in areas of project management, support for training, IT infrastructure and other functions. As part of agile development, the product owner is the sign-off authority for UAT at various relevant stages. In case of other functions, the product owner, his core team and PECMC would be jointly responsible for the following.

7.2.1. Design and development

- Co-ordination with End-user community for gathering requirements.
- Participating in release planning, sprint planning and sprint demo meetings.
- The Product owner will be responsible for maintaining the Product Backlog and prioritizing the items to achieve the goals;
- Clearly express the requirements (including prioritisation) as user stories in the product backlog items;
- Ensure that the Product backlog is visible, transparent and clear so as to ensure the Development Team understands the user stories.
- Re-prioritization of items by the Product Owner at any time;
- Add New items from time to time to the backlog and prioritize as necessary;
- Remove items from the Product Backlog at any time;
- Defining criteria for acceptance of user stories in each sprint.
- Participate in meetings with the Development Team during each Sprint, including to assess developed items;
- Review and provide input for all the deliverables such as Product Backlog, Release Backlog, Sprint Backlog, Sprint Retrospective, Major Release, Product Increments etc., submitted by the Selected Bidder within a defined timeline throughout the implementation phase.
- Review, approve and/or provide recommendations on the change requests identified by the SI.

7.2.2. Acceptance of development

- Identify the UAT team from IA&AD side, who will be executing the User Acceptance Test.
- Report observations to the Selected Bidder and monitor action taken by SI for timely closure of all defects.
- Acceptance in stage 0
  - Code review and review of compliance to coding standards.
  - Document review and sign-off.
  - Sign-off / Acceptance of user stories.
- Acceptance in stage 1 and 2

    - Co-ordination with End-User community for supporting UAT.
    - Code review and review of compliance to coding standards.
    - Document review and sign-off.
    - Sign-off / Acceptance of user stories.
- Review and monitor the completeness of the OIOS Phase 1 and Phase 2 with respect to requirements and performance/acceptance expectations from the solution.
- Review and sign-off “Go-Live”.

7.2.3. Support for Training / capacity building

- Provide the names (nominations) of the personnel to be trained by the Selected Bidder on OIOS system and its components.
- Review and approve Training Plan and Training content prepared by the Selected Bidder for various trainings planned for OIOS System.
- Overseeing the progress of trainings such as Master Trainer training, UAT Training, OIOS System Administration and coordinate signoff activities.
- Review Training results on a periodic basis and provide input on improving the training plan further based upon the feedback received.
- Supporting field audit offices for capacity building.

7.2.4. Project management

- Arranging adequate space and other non-IT facilities in IA&AD premises to the Selected Bidder to deploy the Development Environment and Team members.
- Approving the Integrated Project Management Plan and OIOS Inception Report submitted by the Selected Bidder to implement the OIOS Phase 1 within a defined timeline.
- Approving the project reporting formats submitted by the Selected Bidder to monitor and analyse the progress of the Project.
- Co-ordinate with the Selected Bidder for all the activities needed for successful rollout of the OIOS solution as per the Schedule.
- Apprising the OSC about the progress of the project and report any risk arising.

- Establishing appropriate processes for notifying the Selected Bidder of any deviations from the norms, standards or guidelines at the earliest instance after noticing the same to enable them to take corrective action.
- Review results of post Go-Live workshops conducted by Selected Bidders to understand the overall acceptance of the OIOS System, review and approve remedial actions proposed by the Selected Bidder for increasing the acceptance of OIOS in the User Base.
- Conducting Daily/Weekly / Biweekly / Monthly project review with the Selected Bidder in regards to the progress of the project.
- Facilitate necessary administrative approvals required for setting up Centralized Helpdesk by the Selected Bidder.
- Coordinate with Selected Bidder to ensure successful setting up the Centralized helpdesk with adequate customer support executives and communication facilities.

7.2.5. IT Infrastructure

- Critically review IT resource augmentation requirements proposed by the Selected Bidder at relevant stages/phases of the OIOS project.
- Approve the IT resource augmentation proposed by the Selected Bidder at relevant stages/phases of the OIOS project.
- Reviewing the installation/configuration and deployment of OIOS System and its sub-components in the Tier-3 co-located DC/DR for UAT, Staging, Training and Production environment in both PDC (Primary Data Center), DRC (Disaster recovery Center) and other facilities.
- Infrastructure readiness of field audit offices.
- Coordinating and overseeing procedures for undertaking quality audits of the system on a periodic basis.
- Co-ordinate with the Selected Bidder and third party (if required) for audit of the OIOS system.
- Evaluate and inform about the recommendation of Selected Bidder about the usage of Digital Signatures, and, facilitate the procurement of Digital Signatures for the concerned IA&AD officials, if required.
- Review/monitor the disaster management plans / readiness and mock drills on a periodic basis and oversee the remedial action taken by SI (System Integrator).

- Provide approval on the Incident response and reporting procedure prepared by Selected Bidder. Also monitor adverse incidents reported by the selected bidder.
- Monitor adverse incidents reported by the SI and closely monitor it to closure.
- Review and provide recommendations on the Incident response and reporting procedure prepared by SI.
- Monitor and supervise the activities needed for stabilizing the system and tuning the system for meeting the performance expectations during the early phase of O&M.
- Review patches/upgrades identified by the SI in OIOS application environment.
- Apprising the product owner/ OSC about the acceptance/utilization of the system and report any risk arising.
- Monitor SLAs reporting on a continuous basis along with overall timelines and calculation of penalties accordingly.

7.2.6. Others

- Hand-holding of field audit offices through Level-1 functional help desk.
- Master data readiness.
- Sign-off on data migration strategy and design.
- Support for data migration.

7.3. System Integrator

The major items of responsibility of the SI are listed below. The listing is followed by links to appropriate sections where the responsibility of the SI and requirement of the IA&AD is detailed.

7.3.1. Project Management

- Appoint a project manager.
- He / She will serve as a single-point contact within the institutional framework for the purpose of project monitoring / reporting purposes and shall be deployed by the selected Bidder. He / She will be responsible for all the activities within the OIOS project and will report to Product owner. He/she will be directly responsible for providing periodic project statuses, tasks schedule and Action Taken Reports (ATRs).

- Prepare and submit the Integrated Project Management Plan (IPMP) for implementation of the OIOS Phase 1 to product owner for approval. The IPMP shall comprise of the all the components of deliverables prepared for OIOS Inception and shall adhere to the Scope of work of OIOS system.
- Prepare the project reporting formats to report the progress of the project and submit to product owner for approval.
- Participate in Weekly / Monthly project review in regards to the progress of the project.
- Participate in meeting with OSC, as and when necessary.
- Identify and escalate issues/risks to the Product owner and provide the mitigation plan.
- Adhere to the directions of Product owner as and when provided.
- Prepare and deliver for approval all the deliverables as per Section 7 of One IA&AD System Project RFP volume 2-within a defined timeline, as agreed in the IPMP and to the satisfaction of product owner/OSC, throughout the implementation of OIOS Project.
- Meet all the necessary pre-conditions for system go-live of both OIOS Phase 1 and Phase 2.
- Configure and rollout the OIOS Application in a timely manner as per the schedule defined in the IPMP.
- Provide a periodic report on successful rollout to product owner including justifications for any variance from the finalized rollout plan.
- Prepare exit management plan and get it signed-off by product owner.

7.3.2. IT Infrastructure

- The Selected Bidder shall identify and inform product owner about the usage of Digital Signatures for various officials in the business process workflow.
- Collaborate with the hardware/ software OEMs/ vendors for timely installation of products. Also maintain all kinds of interactions with the service provider of Tier-3 co-located DC/DR and provide regular report to product owner on infrastructure usage, performance and security.
- The SI shall propose the sizing plan of DC/DR for the entire OIOS implementation and Rollout and submit the same to product owner for review and approval. The SI will also submit schedules for gradual ramping up of the IT infrastructure and schedule for a Tech-Refresh to replace the hardware in the Tier-3 co-located DC/DR. Any Resizing in the planned configuration, if required, must be submitted to product owner along with proper justification for approval.

- Procure/Install/configure/deploy all the components (IT and non-IT) of OIOS system and get approval from product owner.

7.3.3. Design and development

Scrum of scrum (of equivalent)

- One of the scrum masters of the parallel development teams is designated as scrum of scrum (or equivalent).
- Ensuring users stories are well understood by the other scrum masters.
- Responsible for co-ordination between the parallel development teams.
- Identify common user stories and inter-related user stories amongst the parallel development teams and facilitate co-ordinated effort to produce an integrated product.
- Ensures user stories meet acceptance criteria of product owner.
- Coordinate with System Integrators of other relevant identified systems such as VLC, IFMS, PFMS, etc., as required, for ensuring that OIOS system seamlessly exchange data with them.
- Identify any patches/upgrades required and report it to product owner and if agreed by product owner, implement the same.
- Identify change requests and report to product owner for necessary action.
- Prepare relevant documentation and get it signed-off by product manager.
- Assist IA&AD and third party for system audit on various parameters, of the OIOS system, if required. IA&AD shall bear the cost of the System Audit.
- Assisting in quality audits of the system as and when required by the product owner.
- Other responsibilities as mentioned in this RFP document.

Scrum master of a development team (or equivalent)

- Design, development and system testing of user stories as per the prioritisation in the backlogs and the requirements signed-off by product owner.
- Ensure UAT readiness of the developed user stories and act upon the feedback received during sprint demo and UAT at various stages.
- Ensure completeness of the OIOS System with respect to meeting functional requirements, performance requirements and the acceptance criteria defined by the product owner and get sign off on the deliverables from the product owner.

Development teams

- Need for parallel development teams to achieve timely delivery of phase 1 and phase 2.
- Responsible for actual development activities with each Sprint.
- Cross-functional – having all the skills needed to create a Product Increment
- Accountable as a team to ensure meeting acceptance criteria of product owner for user stories.

7.3.4. Training and capacity building

- Prepare training plan, required training material/documentation, evaluation methodology to measure learning and execute the training plan as per training requirements of IA&AD.
- Conduct trainings and ensure effective capacity building of the participants.
- Hand-holding support for core team of product owner and empower them to support UAT testing and support during on-boarding of offices other than pilot and nodal offices.

7.3.5. Operations & Maintenance

- Support core team of product owner during the post Go-live.
- Monitor Operations and Maintenance Phase post roll-out of both OIOS Phase 1 and Phase 2.
- Deploy and manage helpdesk and customer support team for addressing the issues and incidents raised by users; resolve such issues and report the status to the product owner on a periodic basis.
- Tune and stabilize the system to meet the performance expectations during all phases based on the System Audit Report of O&M post-go live at no extra cost to IA&AD.
- Prepare an Incident response and reporting procedure and submit the same to product owner for approval. In addition to this, adverse incidents encountered during the Post Go-Live phase need to be prioritized, reported and resolved in a timely manner.
- Prepare SLA report based on the SLA parameters given in RFP Vol III on a continuous basis and submit it to product owner for review and necessary action.
- Prepare and deliver for approval all the deliverables such as Disaster Management Readiness Mock Drill Report, O&M SLA Metrics, Issue Log and Resolutions etc. within a defined timeline, as agreed, and to the satisfaction of product owner, throughout the O&M phase.

8. Scope of Work

The selected bidder shall be responsible for appropriately designing, developing, implementing and maintaining OIOS Application and other project tracks and components for the engagement period. The selected bidder shall design the solution and size the OIOS System as per the scope of work and terms and conditions of the RFP. All tracks / components mentioned in the table below shall be integrated and delivered by selected bidder as part of this project. The architecture in RFP Volume I – Annexure B and Bill of Material specified in the RFP is only indicative. The technical specifications for the various items are provided in a separate document as part of this RFP labeled as **Annexure C: Technical Specifications**

It is the responsibility of the bidder to design the solution in order to meet the functional and non-functional requirements. The bidder may ask for clarification during the preparation of the proposal. The bidder should also clearly specify if the solution proposed does not meet any of the requirements and/or items which are not covered under the scope of the solution. In case, the selected Bidder has not considered any track/component/service which are necessary for the project requirement, as indicated in this RFP, the same shall be brought by the selected bidder at no additional cost to the IA&AD. A summary of tracks relating to scope of work of OIOS project is listed in the table below.

Table 1: Tracks relating to scope of work of OIOS project

Track #	Track Summary
Track 1.	Setting up of development and UAT environment
Track 2.	OIOS Application design, development, roll out and implementation
Track 3.	Setting Up of development, UAT, training, pre-production and production environment in PDC and DRC at Tier-3 co-located data centre.
Track 4.	Centralized helpdesk set up and operations
Track 5.	Training and capacity building
Track 6.	Operations and Maintenance

The scope of work for 6 distinct tracks are further detailed in the narrations below.

8.1. Track 1: Setting up of development and UAT environment

The Phase-I of the OIOS project is envisaged to be rolled out by June 2020. In order to meet this time frame, it is essential that the design and development begin ASAP (Key Resources to be deployed within 15 days, 50% of the Development Team within 3 weeks and 100% of the team within 5 weeks of the date of signing of contract). Considering the minimum turnaround time for setting up and configuring a Tier-3 co-located DC/DR environment for the development and testing environment, the following is proposed.

1. SI shall set up the development and testing environment in a cloud environment.
2. SI shall set up and configure development and testing environment in Tier 3- co-located DC/DR within three months from the signing of contract.
3. SI shall migrate the development and testing environment to Tier-3 co-located DC/DR, as and when it is ready.
4. SI shall set up the remaining environments (training, pre-production and production environment) in Tier-3 DC/DR.
5. SI shall configure Development, testing environment components at cloud, which is identical to the proposed environment at Tier 3- co-located DC/DR; so that its migration/ shifting after 3 months shall need minimum time. The subject migration needs to be planned so as not to lose productivity.

The other activities include the following.

a. **Software Development & Deployment Tools for Continuous Integration and Continuous Delivery (CI/CD):** The SI should Use DevOps toolchain for delivery, development and management of OIOS Application throughout the system development lifecycle. The set of tools for the DevOps toolchain shall be proposed by the SI. The tools should support specific DevOps initiatives such as Plan, Create, Verify, Package, Release, Configure and Monitor.

b. Setup and configuration of system software, supporting platforms and software components (including necessary licenses) that are required for development.

c. Site readiness for Development Center at IA&AD premises.

d. End-user computing devices for SI’s Team

The releases shall be deployed in the test environment for user acceptance testing. Best practices in setting up Development Center should be adopted by the SI so that the Development and Testing zones should be clearly identified and demarcated. The SI shall notify the product owner for all such releases deployed in the test environment and allow selected IA&AD closed user group to perform testing. It would be relevant here to mention that the closed user group of IA&AD would be located in different geographical locations.

Quality processes should be laid out in the Development Center and structured Software Engineering and Project Management practices should be adopted while delivering the OIOS project. The indicative unpriced Rate Card for this track is provided **in RFP Volume II – Appendix I**.

Technical Response from the Bidder in Technical Format 6: The Bidder in the Technical Proposal should propose Bill of Material for setting up the Development and Test Environment. The bidder is at liberty to add any extra item required for successful set up of the environment.

8.2. Track 2: OIOS Application design, development, roll out & Implementation

a. Prescription of the flavor of Agile software development methodology for design, development, testing and implementation of OIOS Software Application.

b. Mandatory Onsite deployment of qualified and experienced resources at Development Center at IA&AD premises Delhi – NCR for Phase 1. The detailed requirements for human resource deployment are provided in **RFP Vol 1, Section 15.**

c. Planning including finalization of Product backlog, release backlog and sprint backlogs.

d. Design, development and testing of OIOS Application services, modules and submodules in a phased manner as per the product / release / sprint backlogs. The modules and sub-modules forming part of Phase 1 and Phase 2 along with Time Phase Development Plan of the Phases thereof are provided in **RFP Vol I, Section 11 : Functional Requirements** in this document. The functional requirement specifications for the modules and sub-modules are further detailed in a separate document as part of this RFP labeled as **'Annexure A: Functional Requirement Specifications for One IA&AD One System Project'.**

e. Procurement, customization and integration of other applications/utilities, as required.

f. **System Testing:** The SI should have a QA/QC process including system testing of each of the user story, to ensure satisfaction of criteria for acceptance, before various stages of User Acceptance Testing. SI will submit System testing report to the IA&AD including the list of test cases, defects identified and resolved before UAT.

g. The Selected Bidder will conduct the sprint demo of each user story of OIOS application from Central premise of IA&AD at Delhi -NCR. The SI should make necessary modifications and code based on feedback received during sprint demo.

h. Deploy OIOS System in the UAT, training and pre-production environments.

i. **User Acceptance Testing:** The acceptance of the user would be measured in the three stages (as described earlier in **Section 5.1.4** in this document).

   (i) Stage 0 (Verification of core functionality)

   (ii) Stage 1 (Validation of core functionality)

   (iii) Stage 2 (Verification & validation of configurability)

   Every stage includes deployment in suitable environments, testing, raising of issues by the Product owner and resolution of issues by the SI. This may be iterated until all issues are resolved. The UAT stage ends with the acceptance by Product owner.

   During the UAT the SI would deploy human resources to support the product owner's team. The co-ordination regarding UAT by geographically distributed pilot and nodal offices would be done by the core team of product owner.

j. **Vulnerability Assessment and Penetration Testing (VAPT):** The SI is responsible to do VAPT of modules/sub-modules released in the respective release (quarter) of each phase by STQC/any Cert-In empaneled agency and submit the VAPT report to the product owner. The SI shall take necessary corrective actions on the suggestions of the product owner.

k. **Testing for sign-off of a phase:** The core team of product owner will conduct a testing for sign-off of a phase for each phase of OIOS application. The sign-off for completion of a phase would be given by the product owner.

l. **Security Audit:** The selected Bidder shall engage STQC or CERT-In empaneled agency to perform Safe to Host Security Audit of each Phase of OIOS Application Go-Live (Phase 1 and 2).

m. **Deployment in pre-production environment:** Walkthrough the modules/sub-modules in a pre-production environment similar to the actual work environment of various IA&AD Offices before final deployment in production environment.

n. **Scheduling of resources:** The resources at the Tier-3 co-located DC/DR would be augmented based on the prescribed schedule for roll out of the OIOS Application releases, as necessary.

o. **Onboarding of offices other than pilot and nodal offices:** After the implementation of the releases in the pilot and the nodal offices, the remaining offices of IA&AD would be on-boarded. This onboarding would be done by the core team of product owner.

The Bill of Material for Track 2 is provided in **'Section** Error! Reference source not found.**:** Error! Reference source not found.**'** of this document.

8.3. Track 3: Setting Up of development, UAT, training, pre-production and production environment in PDC and DRC at Tier-3 co-located data centre

1. Set Up, configure and test **Primary Data Center (PDC)** and **Disaster Recovery Center (DRC)** for each phase of OIOS application in Tier-3 co-located DC/DR.
2. Procure, Provide and Configure Network Connectivity between:
   a. PDC and DRC utilizing two IA&AD NICNET gateways.
3. The above services shall be provided for the project in a phased manner as per the requirements.
4. Procurement, supply, installation, testing and integration of appropriately sized Middleware and System Software in the PDC for each phase of OIOS application. SI should propose appropriate size as per the functional and non-functional requirements for each phase of OIOS application.

5. **OIOS System Sizing for Phase 1 and Phase 2:** The SI should size the entire OIOS Software, System Software, DC/DR components so as to meet the functional and non-functional requirements and SLAs. The SI should adhere to the phased procurement as specified in RFP Volume II. The SLAs are provided in RFP Vol III. The indicative key data points have been provided in **'Annexure D'** to this document.

6. IA&AD intends to implement a data warehousing / data analytics system at a later date for which another service provider will be selected by IA&AD through another RFP. The selected service provider will bring requisite tools, database licenses and other software licenses. The data analytics service provider shall use the servers and centralized storage of OIOS IT solution, which will be augmented by the SI for this purpose at additional cost to be paid by IA&AD by following a change management process. The data analytics system shall be hosted in the same data centre where the OIOS IT solution is hosted. The SI needs to have provision of adding additional rack spaces in the data centre as well as in the DR for hosting the solution. Other common infrastructure of the DC/DR like network, security, bandwidth and other systems as provided by SI shall be leveraged for hosting the data warehousing / data analytics system. The SI will provide separate quote for the rack space hosting charges in its commercial bid. For data analytics system, a separate program needs to be strategized for integrating the results of the analytics to become inputs for audit planning, audit execution and audit reporting. The SI needs to support the data analytics service provider in terms of integration with the OIOS IT solution as per requirements defined at the time of implementation.

The detailed requirements for this track is provided in **'Section 12 : Requirements for setting up DC/DR in Tier-3 Data** Center on CoLo Model**'.** The rate card for Track 2 is provided in RFP Volume II – Appendix I.

8.4. Track 4: Centralized helpdesk set up and operations

1. Set Up and operate a Centralized IA&AD User Helpdesk.

2. Deploy trained resources for Centralized Helpdesk. The detailed requirement for Centralized Helpdesk is elicited in **RFP Vol I Section 14.1 : User Centralized Helpdesk Requirements** in this document**.**

8.5. Track 5: Training and capacity building

This track includes providing the following for training and capacity building as per requirements of IA&AD.

1. Training on agile/scrum methodology (or any another flavor of agile methodology which was prescribed by SI and accepted by product owner) and toolchain to the members the core team of product owner before the commencement of the OIOS Application Phase 1.

2. Training the Master Trainers (identified by IA&AD) for Phase 1, 2 and 3 of OIOS. These master trainers are responsible for training all the employees of their respective field audit offices.

3. Training for UAT team for each release in Phase 1, 2 and 3 of OIOS. The UAT team is responsible for review of the developed user stories at various stages. SI shall also provide training to the members of the core team to support UAT and rollout of OIOS in field audit offices for each quarterly release of the OIOS Application.

4. Training for OIOS System Administration to the identified personnel of IA&AD.

5. Training for team of IA&AD who would discharge functions relating to Level-1 functional desk.

6. Preparation of required training documentation including Batch-Wise Training Schedule, Curriculum, and Training Material.

7. IA&AD to identify trainees and provide training infrastructure.

The bidder shall propose a training team and plan for adequately training the user for adoption of the OIOS System. The detailed requirement is provided in **RFP Vol 1, 'Section 13 : Training and Capacity Building Requirements'** in this document**.**

8.6. Track 6: Operations and Maintenance

The bidder should provide services relating to Operation and Maintenance of the complete OIOS solution and all associated project tracks for a period of **seven** years post OIOS Application Phase 2 Go-live. The detailed requirements are provided in **RFP Vol 1, 'Section 14 : Operations, Maintenance and Security Management Requirements'** in this document**.**

8.7. Common requirements

A. **Resource Deployment:** The detailed requirements relating to requirement of resources of SI and the deployment is provided in **RFP Vol 1, 'Section 15 : resource deployment requirements'** in this document.

B. **Documentation:** Complete documentation of the OIOS Project is required at all relevant stages. The detailed requirements relating to documentation is provided in **RFP Vol 1, 'Section 16 : Documentation Requirements'** in this document**.**

C. **Exit Management Plan:** The Selected Bidder shall provide Exit Management Plan to IA&AD : before System Go-Live of Phase 1 OIOS and Phase 2 OIOS System. The detailed requirement of this plan is elicited in **RFP Vol 1, 'Section 17 : Exit Management Plan and Handover Mechanism'** in this document**.**

D. **Adherence to other requirements:** The following other requirements are detailed in various sections of the RFP document.

   a. Technical/Architecture requirements (RFP Vol I, Section 18)

   b. Non-Functional requirements (RFP Vol I, Section 19)

   c. Project Management requirements (RFP Vol I, Section 20)

   d. Quality requirements (RFP Vol I, Section 21) and

   e. Compliance requirements (RFP Vol I, Section 22)**.**

The definition of "Go Live" is elaborated in **'Section 23'** of this document.

8.8. OIOS Track-wise Responsibility Matrix

Based on the responsibilities listed in **'Section 7'** in this document, the table below indicates the broad set of track-wise activities related to implementation of OIOS Application and responsibilities of these activities.

Track #	OIOS Application Activities	Responsibility
1.	**Setting Up of development and UAT environment**	
	SI shall set up the development and testing environment in a cloud environment.	SI
	SI shall set up and configure development and testing environment in Tier 3- co-located DC/DR within three months from the signing of contract.	SI
	SI shall migrate the development and testing environment from cloud environment to Tier-3 co-located DC/DR, as and when it is ready.	SI
	SI shall set up the remaining environments (training, pre-production and production environment) in Tier-3 DC/DR.	SI
	Software Development & Deployment Tools for Continuous Integration and Continuous Delivery (CI/CD)	SI
	Setup and configuration of system software, supporting platforms and software components (including necessary licenses) that are required for development.	SI
	Site readiness for Development Center at IA&AD premises	IA&AD
	End-user computing devices for SI's Team	SI
2.	**OIOS Application Development, Implementation & Rollout**	

Track #	OIOS Application Activities	Responsibility
	Prescription of the flavour of Agile software development methodology for design, development, testing and implementation of OIOS Software Application.	SI (with consent from product owner)
	Onsite Deployment of qualified and experienced resources at Development Center at IA&AD premises Delhi – NCR for Phase I.	SI
	Planning including finalization of Product backlog, release backlog and sprint backlogs.	SI, Product owner
	Design, Development and Testing of OIOS Application modules, submodules and services in a phased manner as per the product / release / sprint backlogs.	SI
	Procurement, customization and integration of other applications/utilities, as required.	SI
	System Testing	SI
	Walkthrough (sprint demo) of each user story of OIOS application and resolution of issues raised during sprint demo	SI (with review by product owner)
	Deploy OIOS System in the UAT, training and pre-production environments.	SI
	User Acceptance Testing (Stage 0, Stage 1 and Stage 2)	IA&AD
	Resolution of issues raised during UATs (Stage 0, Stage 1 and Stage 2)	SI
	Vulnerability Assessment and Penetration Testing (VAPT)	SI (STQC or CERT-In empanelled agency)

Track #	OIOS Application Activities	Responsibility
	Testing for sign-off of a phase	IA&AD
	Security Audit	SI (STQC or CERT-In empanelled agency)
	On-boarding of offices other than pilot and nodal offices	IA&AD
	Augmentation of resources based on prescribed schedule in the Tier-3 co-located DC/DR	SI (with approval from IA&AD)
3.	**Set Up, Configure & Test of PDC and DRC at Tier-3 co-located DC/DR**	
	Set Up, configure and test Primary Data Center (PDC) and Disaster Recovery Center (DRC) for each phase of OIOS application at Tier-3 co-located DC/DR.	SI
	Procure, Installation, Commissioning and Testing of Storage Area Network (SAN – 10 TB Usable) at two IA&AD Offices along with UPS as NLDC/Backup site.	SI supported by IA&AD
	Procure, Provide and Configure Network Connectivity PDC and DRC utilizing two IA&AD NICNET gateways PDC and 2 IA&AD offices.	SI supported by IA&AD
	Procurement, supply, installation, testing and integration of appropriately sized Middleware and System Software in the PDC for each phase of OIOS application.	SI
	OIOS System Sizing for Phase 1 and Phase 2	SI
4.	**Centralized Helpdesk Set Up and Operations**	

Track #	OIOS Application Activities	Responsibility
	Set Up and operate a Centralized IA&AD User Helpdesk	SI
	Deploy trained resources for Centralized Helpdesk	SI
	Approval of the resumes proposed of the resources before operationalization of Centralized Desk	IA&AD or its nominated agency for approval.
5.	**Training and Capacity Building**	
	Training on agile/scrum methodology and tool chain (or any another flavor of agile methodology which was prescribed by SI and accepted by product owner)	SI
	Master Training to the IA&AD identified Master Trainers for Phase 1, 2 and 3 of OIOS IT solution.	SI
	Training for UAT for phase 1, 2 and 3. Provide training to the members of the core team to support UAT and rollout of OIOS in field audit offices for each quarterly release of the OIOS Application.	SI
	Training for OIOS System Administration to the identified personnel of IA&AD.	SI
	Training for team of IA&AD who would discharge functions relating to Level-1 functional desk.	SI
	Preparation of required training documentation, including batch-wise Training Schedule, Curriculum, and Training Material.	SI (with review and sign-off by IA&AD)
	Identification of Trainees for Training envisaged to act as Master Trainers for IA&AD	IA&AD

Track #	OIOS Application Activities	Responsibility
	Training Infrastructure to be used for training	IA&AD
6.	**Operation and Maintenance of the complete OIOS solution and all associated project tracks for a period of 7 years post OIOS Application Phase 2 go-live.**	SI
7.	**Documentation**	SI (with review and sign-off by IA&AD)
8.	**Exit management plan**	SI (with review and sign-off by IA&AD)
9.	**Adherence to other requirements**	SI

9. Project Timelines: High Level Implementation Timelines of OIOS Project

OIOS project is envisaged to be developed and implemented and rolled out in a staggered manner. The table in the subsequent page provides a high level breakdown of OIOS System into different tracks and phases with corresponding timelines for each tracks and phases thereof. The table also provides development and operationalization of other project tracks along with the timelines.

The legend of the timeline is explained below.

The purple cells represents the duration for which the track would be required.

The brown cells represents the initial commissioning/provisioning of cloud and light brown represents continued provisioning, if necessary.

The light blue cells represent the time period during which the sprints (relating to the release/phase) including planning, design, development, system testing and Stage 0 acceptance testing are envisaged.

The blue cells represent the time period during which the Stage 1 roll-out and acceptance testing is envisaged.

The orange cells represent the time period during which the Stage 2 roll-out and acceptance testing is envisaged.

The green cells represent the time period during which the Stage 3 roll out is envisaged.

The gray cells represent the duration during which Phase 3 development would be taken up.

For the purposes of measuring completion, the last working day of the concerned quarter, as specified in the High-Level implementation timeline, is deemed to be the Project milestone for the relevant milestone for the purpose of this RFP, including the Service Level Agreement. This is applicable for Phases I and II only.

High Level implementation time line of Project Tracks

Track #	Timelines in Years	2020			2020		2021			2021		2022					2023	2023	2024	2025	2026	2027
	Quarters	Q1	Q2		Q3	Q4	Q1	Q2		Q3	Q4	Q1	Q2	Q3	Q4		Q1,Q2	Q3,Q4				Q1,Q2
Track 1	**Set up of development & other environment**																					
	Set up of dev/UAT environment in cloud	🟥	▨																			
	Migration to Tier-3 co-located DC/DR		🟪																			
	All other activities	🟪																				
Track 2	**OIOS Application design, development, rollout & implementation**																					
Phase 1	OIOS Application Phase 1																					
	Design, development & system testing	▦	▦																			
	Stage 0 UAT	▦	▦																			
	Stage 1 UAT (pilot offices)	🟦	🟦																			
	Stage 2 UAT (nodal offices)				🟨	🟨																
	Onboarding of remaining offices						🟩	🟩														
Phase 2	OIOS Application Phase 2																					
	Design, development & system testing				▦	▦	▦															
	Stage 0 UAT				▦	▦	▦															
	Stage 1 UAT (pilot offices)				🟦	🟦	🟦															
	Stage 2 UAT (nodal offices)					🟨	🟨	🟨														
	Onboarding of remaining offices							🟩		🟩	🟩											
Phase 3	OIOS Application Phase 3									▒	▒	▒	▒	▒	▒							
Track 3: Setting Up of development, UAT, training, pre-production / production environment at Tier-3 co-located DC/DR																						
	PDC/DRC for OIOS Phase 1	🟪	🟪																			
	PDC/DRC for OIOS Phase 2				🟪	🟪	🟪	🟪														
	PDC/DRC for OIOS Phase 3									🟪	🟪	🟪	🟪	🟪	🟪							
	NW Setup, NLDC at 2 IA&AD offices	🟪	🟪																			
Track 4	**Helpdesk Setup and Operations**																					
	All activities				🟪	🟪	🟪	🟪		🟪	🟪	🟪	🟪	🟪	🟪		🟪	🟪	🟪	🟪	🟪	🟪
Track 5	**Training and Capacity Building**																					
	Training of product owner's team	🟪																				
	Master Training OIOS Phase 1 and 2	🟪	🟪		🟪	🟪	🟪	🟪														
	UAT Training	🟪	🟪		🟪	🟪	🟪	🟪		🟪	🟪	🟪	🟪	🟪	🟪							
Track 6	**Operations and Maintenance**																					
	OIOS Phase 1 & 2									🟪	🟪	🟪	🟪	🟪	🟪		🟪	🟪	🟪	🟪	🟪	🟪
	OIOS Phase 3										🟪	🟪	🟪	🟪	🟪		🟪	🟪	🟪	🟪	🟪	🟪

10. Engagement Models for Project Tracks & Phases

OIOS is a multi-dimensional project comprising of different project tracks having one or more phase. The engagement model for different phases of each project track is detailed below.

#	Track	Track Items	Engagement Model	Remarks
1.	**Setting Up of Development & UAT environment**	Setting up development & UAT in cloud for three months	Fixed Cost	Three months or until the Tier-3 co-located DC/DR environment is ready and migration is complete
		Migration of development & UAT environment to Tier-3 co-located DC/DR	Fixed cost	
2.	**OIOS Application Development, Implementation & Roll Out**	OIOS Application Phase 1	Fixed Cost	A dedicated development team shall be deployed at IA&AD premises at Delhi-NCR.
		OIOS Application Phase 2	**Fixed cost**	Upon completion of Phase 1, the same team shall continue to the maximum possible extent.
		OIOS Application Phase 3	Time and Material	**Upon** completion of Phase 2, the same team shall continue to the maximum possible extent.
3.	**Setting Up of PDC and DRC at Tier-3 co-located DC/DR**	Tier-3 co-located DC/DR for OIOS Application Phase 1	Phase 1: Fixed Cost	Procure, Provide, Configure and Test the following for PDC and DRC a) System software b) Hardware

#	Track	Track Items	Engagement Model	Remarks
				c) Security d) Disaster Recovery
		Tier-3 co-located DC/DR for OIOS Application Phase 2	Phase 2: Fixed cost	Procure, Provide, Configure bandwidth between PDC, DRC and facilities. The infrastructure deployment should be gradually augmented based on schedule prescribed by SI and approved by IA&AD. The schedule must also provide for a tech refresh.
		Tier-3 co-located DC/DR for OIOS Application Phase 3	Phase 3: Fixed cost	
		Tier-3 Set Up for DRC for OIOS	Fixed cost	
		Tech refresh	Fixed cost	Periodicity to be determined
		Backup Sites	Fixed cost	At 2 IA&AD offices
4.	**Track 4: Centralized Helpdesk Set Up and Operations**	a. Helpdesk Tool b. Helpdesk Resources	Time & Material for Resources	A separate and dedicated team shall be deployed for operating the Centralized IA&AD helpdesk
5.	**Track 5: Training and Capacity Building**		Time & Material for each Training conducted	
6.	**Track 6: Operations & Maintenance**	OIOS Application Phase 1 and Phase 2	Fixed Cost	
		OIOS Application Phase 3	Time & Material	

11. Functional Requirements

The OIOS IT solution is to be designed, developed, tested, implemented and rolled out to the various field audit Offices. The envisaged business process in OIOS ecosystem is bundled into modules and sub-modules of "business value". The functional requirements for each of the modules/sub-modules are elaborated in '**Annexure A: Functional requirement specifications for OIOS**' to this document. Therefore, the IT solution is envisaged to be rolled out in three phases. In addition, the architecture should be scalable to allow IA&AD to add new modules and services, as necessitated by future requirements beyond Phase 1 and Phase 2 or further phases of IA&AD. The selected bidder should be able to deliver at the minimum, the functional services as listed in sections below. The non-functional Requirements are provided in **'Section 19'** of this RFP document.

11.1. High level Functional Overview of services

The Overall scope of OIOS Application is divided into a number of interrelated services, modules, and submodules. The OIOS IT application is intended to provide the following business services.

a) **Audit and related services:** These are services relating to core audit processes. The modules include,

- Audit planning of audit assignments.
- Detailed audit design of the audit assignments.
- Execution of the audit plan and design and collection of data.
- Reporting of findings observed during execution and recommendations made thereafter.
- Follow-up on action taken on products containing findings and recommendations.
- Technical Guidance & Support services.
- Services offered by inspection wing, peer offices through review and internal audit.

b) **Non-audit services:** These are peripheral services that support the core audit services. The modules include,

- Administrative services (Non-HR related).

c) **Master data services:** These are services that assist management of master data relating to the audit and non-audit services. The modules include,

- Organisational structure of the department and the field audit offices.

- Personnel engaged in various activities of the department.
- Universe of auditable entities (similar to clients of IA&AD's business).

d) **Common services:** These are services commonly used by all the other services. The modules include,

- Platform based collection of data required by other services or during delivery of other services.
- Communication service.
- Reporting and dashboard services.
- Institutional management of knowledge.
- Migration of legacy data.

The schematic below provides a high-level overview of the services (and modules) offered by the envisioned OIOS Application.

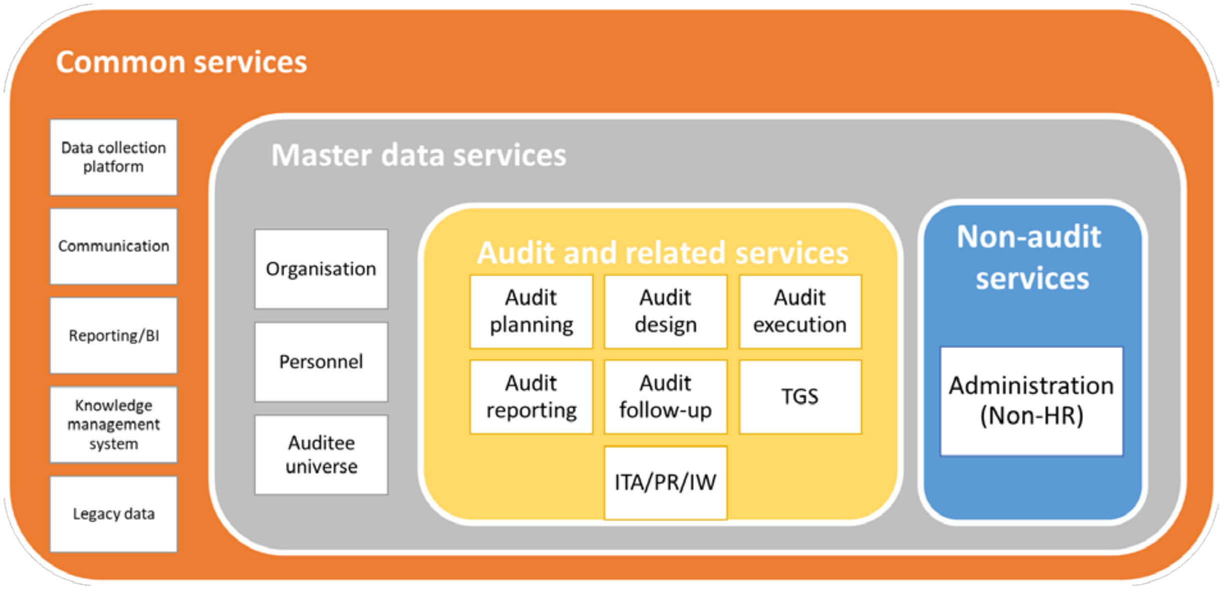


Figure 6: OIOS IT solution (Services and modules)

11.2. Time Phase Development Plan for OIOS Application

The overall scope of OIOS Application is divided into a number of interrelated services, modules and submodules which should be juxtaposed in an orderly fashion to sequentially evolve the OIOS application into a robust IT solution. This will be achieved by architecting the proposed solution into three phases containing quarterly release (bundles) of said services, modules and submodules. The phase-wise bundling the modules/sub-modules is detailed below. It is important to note that the bundling of modules/sub-modules are indicative and would be finalised during the release planning based on estimate for each sub-module in product backlog.

<table>
<tr><th colspan="6">Phase-wise bundling of development of modules and sub-modules of services (release)</th></tr>
<tr><th colspan="6">Phase I of OIOS</th></tr>
<tr><th colspan="3">Release 1</th><th colspan="3">Release 2</th></tr>
<tr><td colspan="3"><b>Module 01: Organisation</b>
• Office master
• Office structure
• User privilege master**
• User roles
• Role-structure map
<b>Module 02: Personnel</b>
• Employee master
• Posting/transfer
<b>Module 03: Auditee universe</b>
• Universe master
<b>Module 06: Audit Execution</b>
• Audit toolkit (Collect) platform (part)
<b>Module 09: Data collection</b>
• Design kit
• Allocate access
• Monitor collection
• Consolidate & analyse
<b>Module 12: Knowledge management system</b>
• Audit guidance (part)
• Auditee IS (part)</td><td colspan="3"><b>Module 02: Personnel</b>
• Gradation list
<b>Module 04: Audit planning</b>
• Annual audit plan
<b>Module 05: Audit design</b>
• Audit design matrix
• Sampling approach
• Audit guidelines
<b>Module 06: Audit execution</b>
• Programme
• Record requisition
• Audit enquiry
• Audit observation
• Audit toolkit (collect) platform (part)
<b>Module 07: Audit reporting</b>
• Product configuration (part)
• Drafting product (part)
<b>Module 12: Knowledge management system</b>
• Audit guidance (part)
• Auditee IS (part)
<b>Module 13: Reporting/BI</b>
• MIS reports**
• Dashboards**</td></tr>
<tr><th colspan="6">Phase 2 of OIOS
(<b>Note:</b> Release 6 only involves changes that are added due to Stage 2 UAT)</th></tr>
<tr><th colspan="2">Release 3</th><th colspan="2">Release 4</th><th colspan="2">Release 5</th></tr>
<tr><td colspan="2"><b>Module 03: Auditee Universe</b>
• Universe profile
<b>Module 06: Audit execution</b>
• Offline utility (part)
<b>Module 07: Audit reporting</b>
• Product config (part)
• Drafting product (part)
• QA/QC of audit product
• Finalisation & issue
<b>Module 10: Communication</b>
• Receipt
• Dispatch</td><td colspan="2"><b>Module 02: Personnel</b>
• Employee profile
<b>Module 06: Audit execution</b>
• Offline utility (part)
<b>Module 07: Audit reporting</b>
• Receive response
<b>Module 08: Audit follow-up</b>
• IR follow-up
• LC follow-up
<b>Module 13: Reporting/BI</b>
• MIS reports**
• Dashboards**</td><td colspan="2"><b>Module 02: Personnel</b>
• Training nominations
• Other nominations
<b>Module 04: Audit planning</b>
• Parametric risk
<b>Module 07: Audit reporting</b>
• Recommendations
<b>Module 08: Audit follow-up</b>
• Reco. follow-up
<b>Module 12: KMS</b>
• Repository of ADM/TK
• Forum</td></tr>
</table>

Phase-wise bundling of development of modules and sub-modules of services (release)		
• Notification / Alert **Module 13: Reporting/BI** • MIS reports** • Dashboards** **Module 16: Legacy data** • Bulk data migration • Adhoc data entry		• Wiki • Media repository
Phase 3 of OIOS		
Bundle A	**Bundle B**	**Bundle C**
Module 04: Audit planning • Strategic audit plan **Module 05: Audit design** • Statistical sampling **Module 12: KMS** • Instant messaging **Module 15: Administration** • RTI • Complaints	**Module 02: Personnel** • Leave • Tour • Personnel Claims **Module 06: Audit execution** • API integration **Module 07: Audit reporting** • API integration **Module 08: Audit follow-up** • API integration **Module 14: TGS** • TGS • LB Committee	**Module 11: ITA/PR/IW** • Internal test audit • Peer review • Inspection wing **Module 15: Administration** • Procurement • Asset • Inventory
**** These sub-modules would evolve and/or change with every release.**		

11.3. Staging of implementation in each phase

The staging of the implementation and roll out (Stages 1, 2 and 3) is detailed out in ‘Annexure A: Functional requirement Specifications’ of this document. The same is replicated in this document for ease of reference. It is important to note that the staging of the modules/sub-modules are indicative and would be finalised during the release planning based on estimate for each sub-module in product backlog.

In respect of phase 1 and phase 2, the sub-modules would be implemented in three stages (after adequate testing) as detailed below. However, in respect of phase 3, the implementation of sub-modules would be an all-India level after adequate testing.

Stage 1: Development & Proof of core functionality: The sub-module functionality is envisaged to be developed and implemented in a few selected field audit offices (four to five) with an objective to validate the design at a basic level. The purpose is to validate the core functionality. This is the first stage of acceptance. This is denoted by blue colour.

Stage 2: Proof of ability to configure: The sub-module is envisaged to be implemented in the selected 31 pilot offices (excluding offices already covered in the proof of concept) and their respective functional wings in C&AG HQ covering a variety of audit streams. The objective of pilot implementation is to validate the applicability of the design across audit streams and validate the configurability features. This is the second stage of acceptance. This is denoted by orange colour. Any changes made in the requirements subsequently, after stage 2, would be taken up as a change request.

The feedback received during testing of stage 1 and stage 2 would be considered 'within scope' of the RFP. That is, Additional story points or changes in story points that are added based on feedback received in stages 1 and 2 would **NOT** be considered as '**change management**'.

Stage 3: All-India implementation: The sub-module is envisaged to be implemented in all field audit offices and the sub-module reaches an irreversible status. At this stage, only configuration (and not change management/ customization) is expected, since the validation of configurability features has already been confirmed in the pilot implementation. This is denoted by green colour. Any changes required based on the feedback received during stage 3 (for sub-modules covered under phases 1 and 2) would be handled as a '**change management**'.

Phase 1 and 2: The sub-modules to be developed and implemented in phase 1 and 2 have been divided into **eight** (indicative) releases. The releases are indicated with numbers in the cells of the table. Further, the road map also includes the extent of coverage in IA&AD, as detailed below.

Phase 3: The sub-modules to be developed and implemented in phase 3 have been bundled into three bundles (A, B and C). The bundle number has been indicated against the sub-modules to be developed in phase 3.

The complete information discussed above is illustrated in the infographic below. The sub-modules marked with ** would undergo modification until completion of phase 3. One sub-module (Auditee data warehouse) which would be handled independently is highlighted in black.

Table 2: Timelines for stage-wise implementation of sub-modules of OIOS (Road map)

	Phase 1		Phase 2				Phase 3 (T&M)						>>
Year	2020				2021				2022				>>
Quarter	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	>>
01: Organisation													>>
01_01: Office Master	1	2	3	4	5								>>
01_02: Office structure	1	2	3	4	5								>>
01_03: Privilege master**	1	2	3	4	5								>>
01_04: User roles	1	2	3	4	5								>>
01_05: Role-structure map	1	2	3	4	5								>>
02: Personnel													>>
02_01: Employee master	1	2	3	4	5								>>
02_02: Employee profile				4	5	6	7						>>
02_03: Posting/Transfer	1	2	3	4	5								>>
02_04: Gradation list		2	3	4	5								>>
02_05: Training					5	6	7	8					>>
02_06: Other nominations					5	6	7	8					>>
02_07: Leave									B	B			>>
02_08: Tour									B	B			>>
02_09: Personnel claim									B	B			>>
03: Auditee Universe													>>
03_01: Universe master	1	2	3	4	5								>>
03_02: Universe profile			3	4	5	6	7						>>
04: Audit planning													>>
04_01: Strategic Audit plan							A	A					>>
04_02: Annual Audit plan		2	3	4	5	6							>>
04_03: Parametric risk					5	6	7	8					>>
05: Audit Design													>>
05_01: Audit Design Matrix		2	3	4	5	6							>>
05_02: Sampling approach		2	3	4	5	6							>>
05_03: Audit guidelines		2	3	4	5	6							>>
05_04: Statistical sampling							A	A					>>
06: Audit execution													>>
06_01: Programme		2	3	4	5	6							>>
06_02: Record requisition		2	3	4	5	6							>>
06_03: Audit enquiry		2	3	4	5	6							>>
06_04: Audit observation		2	3	4	5	6							>>
06_05: TK-collect platform	1	2	3	4	5	6							>>
06_06: API Integration									B	B			>>
06_07: Offline utility			3	4	5	6	7						>>
07: Audit reporting													>>
07_01: Product configuration		2	3	4	5	6	7						>>
07_02: Drafting audit product		2	3	4	5	6	7						>>
07_03: QA/QC			3	4	5	6	7						>>
07_04: Finalisation & issue			3	4	5	6	7						>>

	Phase 1		Phase 2				Phase 3 (T&M)						>>
Year	2020				2021				2022				>>
Quarter	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	>>
07_05: Receive response				4	5	6	7	8					>>
07_06: Recommendations					5	6	7	8					>>
07_07: API Integration									B	B			>>
08: Audit follow-up													>>
08_01: IR follow-up				4	5	6	7	8					>>
08_02: LC follow-up				4	5	6	7	8					>>
08_03: API Integration									B	B			>>
08_04: Reco follow-up					5	6	7	8					
09: Data collection platform													>>
09_01: Design kit	1	2	3	4	5								>>
09_02: Allocate access	1	2	3	4	5								>>
09_03: Monitor collection	1	2	3	4	5								>>
09_04: Consolidate & Analyse	1	2	3	4	5								>>
10: Communication													>>
10_01: Receipt			3	4	5	6	7						>>
10_02: Dispatch			3	4	5	6	7						>>
10_03: Notification / Alert			3	4	5	6	7						>>
11: ITA/PR/IW													>>
11_01: Internal test audit											C	C	>>
11_02: Peer review											C	C	>>
11_03: Inspection wing											C	C	>>
12: KMS													>>
12_01: Audit guidance	1	2	3	4	5								>>
12_02: Auditee IS	1	2	3	4	5								>>
12_03: Repository of ADM/TK					5	6	7	8					>>
12_04: DW/data analytics	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	>>
12_05: Forum					5	6	7						>>
12_06: Wiki					5	6	7						>>
12_07: Media repository					5	6	7						>>
12_08: Instant messaging							A	A					>>
13: Reporting/BI													>>
13_01: MIS reports**		2	3	4	5	6	7	8					>>
13_02: Dashboards**		2	3	4	5	6	7	8					>>
14: TGS													>>
14_01: TGS									B	B			>>
14_02: LB Committee									B	B			>>
15: Administration													>>
15_01: Procurement											C	C	>>
15_02: Asset											C	C	>>
15_03: Inventory											C	C	>>
15_04: RTI							A	A					>>
15_05: Complaints							A	A					>>

	Phase 1		Phase 2				Phase 3 (T&M)						>>
Year	2020				2021				2022				>>
Quarter	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	>>
16: Legacy data													>>
16_01: Bulk data migration			3	4	5	6	7	8					>>
16_02: Adhoc data entry			3	4	5	6	7	8					>>

11.4. Functional requirement specifications

The functional requirement specifications of OIOS for modules and sub-modules to be developed in Phase 1 and Phase 2 of OIOS project, are elaborated in **"Annexure A: Functional requirement specifications of OIOS IT solution"** to his document**.** The bidders are suggested to go through the requirements thoroughly.

Please note that the requirements detailed in the functions Requirements will necessarily have to be met by the system designed and developed by the SI, and the approval of any intermediate document during the course of the project will not nullify any specification entailed in the Phase 1 and Phase 2 functional requirements, unless explicitly stated.

11.5. Special requirements for Phase 3 Modules

The overview of functional requirement specifications of modules and sub-modules to be developed in Phase 3 of OIOS project are also provided in **"Annexure A: Functional requirement specifications of OIOS IT solution".** The Bidders are suggested to go through the requirements thoroughly.

The functional requirements for Phase 3 modules, sub-modules and services would evolve and shall be finalized before the completion of Phase 2. It is made clear that the SI's team shall work along with the IA&AD team and its nominated agency to finalize such requirements and the same shall be developed, implemented and rolled out in the IA&AD offices on T&M basis.

12. Requirements for setting up DC/DR in Tier-3 Data Center on CoLo Model

The selected bidder shall provision, configure and test the following in Tier-3 co-located DC/DR in a phased manner as per Implementation Timelines

1. System Software
2. Hardware
3. Security
4. Disaster Recovery

In addition to the above, the selected bidder shall also provision, configure Bandwidth Connectivity between DC and DRC, NICNET Gateway-1 and 2.

12.1. Role of Selected Bidder

- Appropriately size the infrastructure requirement as per the requirements of the current track, or rollout requirements.
- Host the OIOS Application in the both Primary Data Center and Disaster Recovery Center.
- Test and ensure the SLAs are complied with.
- DRC:
  - Make provision for 50% compute of Primary Data Center (as per RFP Volume I – Annexure C)
  - Make provision for 100% identical storage of Primary Data Center (as per RFP Volume I – Annexure C)
  - Make provision for necessary system software
- Create, operate and maintain the development, UAT, training, pre-prod and production environments for a duration of
  - three or more years from the start date of OIOS and until the development and roll-out of Phase 3 and
  - seven years from the "Go-Live" satisfying the requirements detailed below.

12.1.1. IT infrastructure procurement, supply and installation

a. SI shall be responsible for procurement, supply and installation of entire IT infrastructure required for setting up, operating and maintaining the OIOS IT solution.

b. The IT infrastructure includes servers, storages, back up, networking, security equipment, operating systems, database, help desk system and other related infrastructure required for running and operating the OIOS IT solution.

c. The planning of IT infrastructure procurement should consider the following factors.

    a. Ensure redundancy at each level.

    b. Support peak loads.

d. SI shall plan procurement of infrastructure in a staggered manner during the project duration to support increase in number of offices being on-boarded and increase in data. The SI shall propose staggered procurement schedule and provide commercial quotation accordingly including the scope for tech refresh.

e. The SI shall procure infrastructure in a phased manner based on the prescribed schedule as provided in RFP Volume II Appendix I and after receipt of approval from product owner.

f. Virtualization technologies shall be used to reduce the physical space required for hosting.

g. IT infrastructure shall be dedicated for OIOS project and SI shall not use the same for any other purpose.

h. In case of procurement of infrastructure in phases, the payment for the same shall also be made in phases after actual delivery and acceptance of such infrastructure in specified locations. Title transfer of hardware and system software shall take place after commissioning of respective components and acceptance by IA&AD.

i. The initial estimate for procurement of infrastructure may be planned based on the indicative key data points detailed in '**Annexure D: Indicative key data points**' to this document.

j. SI shall provide details and quote charges for additional compute (server, storage and related infrastructure items) that would be required on a year-on-year basis after the Go-Live. The networking and security components may be sized suitably as well to meet the requirements defined in SLA.

k. SI shall ensure to procure warranties/ AMCs for the all the hardware components for the entire duration of the project.

l. SI shall obtain support from OEM for software component.

m. The minimum specifications of IT infrastructure and information security are detailed in Annexure C. The SI shall size and provide IT infrastructure to meet the functional and non-functional requirements and the Service Level Agreement parameters.

n. The bidder shall prepare and submit the details of methodology and computations for sizing and capacity of storage, compute, routers, switches, internet facing IPS, backup, tape libraries, security components along with their technical proposal, including schedule for gradual on-boarding and tech refresh.

12.2. Hosting requirements

a. Bidder shall enter into a tri-party agreement with Data Center Service Provider and IA&AD for required Data Center Services, however sole responsibility to provide the services as per the RFP requirements shall lie with SI

b. The agreement between SI and Data Center Service Provider must be in line with the SLAs defined in the RFP.

c. Rental charges for various services offered by Data Center Service Provider for Project duration must be added in the Commercial Proposal and it shall be added in total Project bid value for evaluation purpose.

d. SI shall provide space and required infrastructure, including, provisioning for required bandwidth for hosting all the components of OIOS IT solution.

e. The OIOS IT solution shall be hosted in a commercial tier 3 data centre in India.

f. The Disaster Recovery site will also be required to be hosted in a commercial tier 3 data centre in a different location that mitigates the risk of both sites being affected by location specific threats.

g. For each of the site (DC & DR) there has to be Near DC/Near DR, which will be hosted at IA&AD provided space in the same city. No other compute infrastructure except storage, UPS is proposed to be hosted at these sites.

h. The proposed DC/DR should be compliant to Tier 3 standards.

i. The hosted IT infrastructure in the facilities of DC/DR shall be housed in a separate caged environment dedicated to IA&AD at each site. The cage should have biometric based access along with facility to put lock and key.

j. The SI shall make the access logs relating to the access for the cage using biometric available every 60 days. The SI shall also provide for video surveillance for the entrance as well as the perimeter of the cage. The video surveillance shall be available for at least 30 days. The live video feed for each of the camera may be made available for viewing at IA&AD premises on real time basis. For this purpose, the internet connectivity at IA&AD premises will be procured by IA&AD. However, connectivity requirement at camera end to be borne by SI.

k. DC and DR facilities should have existing and valid ISO 27001 certified. The certificate shall be maintained by the service provider for the DC/DR facilities during the entire duration of the contract.

l. SI shall ensure sufficient electrical connections, air conditioning, backup power through generators, access control, integrated fire detection and suppression, physical security and soft services, etc., as applicable and required for the proposed infrastructure on a 24 x 7 basis in order maintain the availability of all the facilities as per SLA.

m. SI shall also provider for common security devices such as door sensors, staff attendance control systems, video surveillance, monitoring, recording facilities, etc.

n. The facilities should have common space available along with other infrastructure like lifts, building management system, electrical systems, security systems, fire alarm and suppression systems, heat ventilation and precision air-conditioning-based cooling system adequate to handle cooling requirements for equipment hosted. All the aforesaid infrastructure should be integrated to a central building management system to provide better infrastructure control.

o. SI shall evaluate the sizing of rack space required at the facilities for the entire duration of the contract with adequate space for future expansion and scalability requirements. The future requirement for hosting the data warehouse/data analytics system shall also be kept in mind. The payment relating to the hosting charges for the data warehouse/data analytics system including power charges and rack cost shall be paid additionally by IA&AD from the date when the IT infrastructure is hosted in these racks by IA&AD.

p. The technical proposal of the SI shall provide year-wise details on the number of racks that the SI intends to host at each facility along with the IT infrastructure deployment plan for each rack and the rated power considered for each rack. The racks and the required cabling shall be procured and installed by SI.

q. The power distribution system in these facilities should ensure that addition or removal of any equipment or component does not involve power interruption.

r. SI shall provide for two levels of manned security. The first level at the complex entry (for perimeter security) and second level at the main data centre control (for visitor control).

s. SI shall not change the hosting provider during the contract duration, without prior approval of IA&AD.

t. Facilities proposed for DC, DR, Near DC and Near DR should additionally meet the parameters mentioned in RFP Volume I - Annexure C. Compliance to these parameters also need to be submitted along with the technical proposal.

u. During working hours (0900-1800 hrs) at least one resource from the SI's Infrastructure team should be deployed at both DC locations for the entire contract period.

v. The implementation must ensure that necessary backup copies are valid and can be successfully restored, which requires ranking the importance of data and establish ways that the most important data is backed up first and restored first. The ranking of importance of Data shall be submitted by SI to the IA&AD and shall be implemented after IA&AD's approval.

12.2.1. Bandwidth requirements

a. SI shall provide MPLS connectivity for connecting NIC gateway with the DC and DR facilities.

b. SI shall provide MPLS connectivity between DC/DR/Near DC/Near DR to meet the required RPO and RTO. This should include the following.

    a. Connectivity between DC and DR.

    b. Connectivity between DC and Near DC.

    c. Connectivity between DR and Near DR.

    d. Connectivity between DR and Near DC.

    e. Connectivity between DC and Near DR.

c. SI shall also provide for internet connectivity at DC/DR to allow the OIOS IT solution to be accessible from internet. Internet connectivity needs to be provided from ISPs at each data centre. The internet bandwidth should be provisioned to meet the user requirements.

    a. IA&AD officials accessing OIOS IT solution through NIC-NET.

    b. IA&AD officials accessing OIOS IT solution from elsewhere.

    c. Any other entities accessing the system through portal/APIs.

d. SI shall ensure connectivity to helpdesk team and O&M team.

e. The estimation of bandwidth shall be done by SI based on the data replication requirements and indicative key data points detailed in **'Annexure D'** to this document. The SI shall ensure scalability requirements as well and ensure to meet SLAs.

f. The bandwidth calculation should ensure that the utilization does not exceed 70% at any point of time. If the bandwidth reaches 70%, the SI shall increase the bandwidth without any additional cost to IA&AD.

g. The SI shall provide details of bandwidth service provider.

h. The SI through EMS should provide for network reports including

    a. Link up/down (real-time plus periodic)

    b. Link utilization (real-time plus periodic)

    c. Bandwidth utilization report.

    d. Application/port level traffic analysis.

    e. Reports relating to jitters and network latency

    f. Router statistics.

    g. Memory and CPU utilization

12.2.2. Other Requirements

1. Each of the environments mentioned above should be logically isolated, i.e., separate from the production environment in a different VLAN than the production environment and setup such that users of the environments are in separate networks.

2. The selected bidder should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system states, databases and enterprise applications as per the backup policy.

    a. SI shall provide for fireproof media storage for storage of tapes, cartridges, etc.

    b. Backup solutions for Production, DR and Staging in the form of disk to disk to tape or latest generation LTO (One Copy).

    c. Bidder has to provide a dedicated or shared backup tool for backup of the Database, Applications etc. The backup has to be automated through backup agents

    d. Backup of production will be daily incremental, weekly full and monthly full. The period of retention of backups for weekly will be 30 days and for monthly backups will be 90 days.

    e. Bidder has to ensure the data backup for DR and staging on weekly basis and data retention period will be 30 days.

f. The Bidder shall perform restoration test every Quarter on a separate VM and provide suitable reports.

g. All backups have to be completed between a 6-hour window i.e. between 12 AM to 6 AM.

3. The database server storage has to be provided on high speed disks (SSD's) for better performance.

4. Bidder has to provide Private static IP address for all the VM's and provide minimum of 10 Public IP address in DC and DR respectively.

5. The SI has to provision VPN gateway for accessing the Servers for troubleshooting. The connectivity has to be provided for 5 clients for troubleshooting issues. The internet connectivity required for VPN has to be separately provisioned.

6. DRC should meet all the requirements as specified in Annexure C of this document.

7. RTO and RPO should be as per Disaster Recovery and Business Continuity Requirements as specified in Annexure C of this RFP.

8. DR drills need to be performed by the Bidder half yearly and/or on demand basis to check disaster preparedness.

9. Compliance process to the defined international standards and security guidelines such as ISO 27001, for maintaining operations of cloud and ensuring privacy of IA&AD data.

10. A change release management and configuration management procedure is defined and implemented to process any change to the services. This procedure must include the capability to support the transition between the aforementioned environments prior to production deployment.

11. The infrastructure provisioned by the Bidder must be scalable.

12. The Bidder shall conduct vulnerability and penetration testing (from third party agency empanelled with CERT-In/ STQC) on the facility every year and the report should be shared with IA&AD. The Bidder would ensure that the updates are made to the systems in response to any adverse findings in the report; without any additional cost to IA&AD.

13. Provide support to technical team of IA&AD or nominated agency for Optimization of resources for better performance and also provide physical and virtual access to the technical persons for the resolution of any issue pertaining to the operation, maintenance or

rectification to keep the application running without any problem, as authenticated by IA&AD.

14. The SI shall provide 24*7 Helpdesk & Technical support services. This will include system maintenance windows. The service provider should provide a 24*7 operated contact number which will be used by IA&AD or by IA&AD nominated partners to raise any issues related to the services provided by the bidder.

12.2.3. Certification/Compliance

i. The facilities/services for both Primary Data Center and Disaster Recovery Center need to be certified / compliant for the entire duration of the contract to the following standards based on the project requirements:
   a. ISO 27001 - the services should be certified for the latest version of the standards
   b. ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology

ii. The SI shall meet all the security requirements indicated in the IT Act 2000.

iii. The bidder shall submit the respective certificates issued by the authorized agency/persons to IA&AD

12.2.4. Privacy and Security Safeguards

1. The Bidder shall ensure that the data is encrypted as part of a standard security process for highly sensitive content or choose the right cryptographic algorithms evaluating security, performance, and compliance requirements specific to their application and may choose from multiple key management options. Refer Annexure A for functional requirement.
2. SI shall notify IA&AD promptly in the event of security incidents or intrusions, or requests from foreign Government/Non-Government agencies for access to the data, to enable the IA&AD to manage these events proactively.
3. The SI shall report forthwith in writing of information security breaches to the IA&AD by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential Information.

4. The SI shall ensure to treat information passed on to them under this Agreement as classified. Such Information will not be communicated / published / advertised by the SI to any person/organization without the explicit permission of the IA&AD.

12.2.5. Confidentiality

1. The Bidder shall execute non-disclosure agreements with the IA&AD with respect to IA&AD confidentiality of OIOS and / or IA&AD data.
2. For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:
   a) information already available in the public domain;
   b) information which has been developed independently by the Service Provider;
   c) information which has been received from a third party who had the right to disclose the aforesaid information;
   d) Information which has been disclosed to the public pursuant to a court order.
3. The SI shall ensure that the service provider does not get access to IA&AD data.
4. The bidder remains responsible for its subcontractors' compliance with bidder's obligations under the Project.

12.2.6. Performance Management

The SLAs for DC/DR services are covered under RFP Vol 3.

12.2.7. Audit & Governance Requirements

The SI shall implement the audit & compliance features to enable the IA&AD to monitor the provisioned resources, performance, resource utilization, and security compliance:

i. View into the performance and availability of the services being used, as well as alerts that are automatically triggered by changes in the health of those services.

ii. Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure.

iii. System-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms).

iv. Logs of all user activity within an account. The recorded information should include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the service. This is required to enable security analysis, resource change tracking, and compliance auditing.

v. Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered each time a configuration changes, and Agencies should be given the ability to dig into the configuration history to perform incident analysis.

vi. Monitoring of resources with alerts to customers on security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using Identity and Access Management (IDAM), and weak password policies.

vii. Automated security assessment service that helps improve the security and compliance of applications by automatically assessing applications for vulnerabilities or deviations from best practices. After performing an assessment, the tools should produce a detailed list of security findings prioritized by level of severity.

12.3. Exit Management / Transition Requirements

Continuity and performance of the Services at all times including the duration of the Agreement and post expiry of the Agreement is a critical requirement of IA&AD. It is the prime responsibility of SI to ensure continuity of service at all times of the Agreement including exit management period (three months). SI shall ensure the continuity during transition period and in no way any facility/services shall be affected/degraded.

Amongst others, a service provider could be changed/decommissioned subject to the following two triggers as explained below:

1. **Non-performance:** The performance will be monitored against set SLAs and if the service provider fails to meet the SLAs for two consecutive quarters the SI shall migrate to a different service provider at no extra cost and ensure the SLAs are met with the new service provider.

2. **Material breach:** In case of a data breach resulting in material breach, the IA&AD have rights to terminate both SI and service provider on an immediate basis along with revoking the PBG submitted by SI.

The responsibilities of service provider with respect to Exit Management / Transition-Out services include:

a. Provide necessary handholding and transition support to ensure the continuity and performance of the Services to the complete satisfaction of IA&AD.
b. Support IA&AD in migration of the infrastructure, data, content and any other assets to the new environment created by IA&AD or any Agency (on behalf of IA&AD on alternate service provider's offerings to enable successful deployment and running of the IA&ADs solution on the new infrastructure by providing a mechanism to IA&AD for the bulk retrieval of all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to IA&AD supplied industry standard media.
c. The format of the data transmitted from the service provider to IA&AD should leverage standard data formats whenever possible to ease and enhance portability.
d. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with IA&AD.
e. Ensure that all the documentation required by IA&AD for smooth transition including configuration documents are kept up to date and all such documentation is handed over to IA&AD during regular intervals as well as during the exit management process.
f. Shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of IA&AD.
g. Once the exit process is completed, remove the **IA&AD'***s* data, content and other assets from the environment and certify that the infrastructure, Content and data destruction to IA&AD as per stipulations and shall ensure that the data cannot be forensically recovered.
h. There shall not be any additional cost associated with the Exit / Transition-out process.

13. Training and Capacity Building Requirements

Training and Capacity Building is a critical component for the adoption of OIOS system. The purpose of this initiative is to equip the end-users and other stakeholders of OIOS system with the right skills, and knowledge to use OIOS and achieve its objectives in terms of enhancing outcomes in Audit Planning, Execution, Reporting and other audit functions. This component is critical to the sustainability of use of the OIOS IT solution by the end-user community.

The Selected Bidder will be responsible for creation of a detailed and effective training strategy, user groups and classifications, training plan and guidelines, detailed training material, training program designed their delivery to the target users. The selected bidder will also be responsible for drawing out an effective methodology for evaluation for each training and to measure the effectiveness of the training. The training and capacity building requirements are detailed in the sections below. Any additional training requirement/requirement of additional batches would be taken up on a time & material basis based on the rates provided by the bidder.

The core components of training will have to be delivered using the SI's own resources; however, SI can consider using sub-contracting for part of the training and capacity building requirements as part of the overall Training Plan after prior approval of the IA&AD.

13.1. Training / capacity building of product owner's core team

The bidder has to provide training for the product owner's core team in the following areas.

#	Training Type	Number of Trainees	Batch Size	Number of Batches	Number of Days per batch
1.	Agile methodology Training	20	10	2	2
2.	Tool chain training	20	10	2	3
3.	Training on the functional help desk tool	15	5	3	3

13.2. Training of Master Trainers

The majority of the master trainers are a set of two to three officials of IA&AD from each of the 141 field audit offices. The trainers have to be imparted training in office administration, wing administration and functions and activities to be carried out by other officials in the office. The Trainees identified by IA&AD for Training are envisaged to act as Master Trainers for IA&AD. Upon successful training these Master Trainers are envisaged to become trainers for their own respective office. It, therefore, becomes imperative on the selected bidder to impart effective training to such Master Trainers.

The officials of IA&AD in each of the field audit offices vary widely with regard to IT skills and capacity. It is very important that the master trainers become Subject Matter Experts with respect to using the OIOS IT solution, so that they can hand hold and assist the other officials in their respective offices throughout the journey of implementation. The training material for these trainings must be carefully designed so that it is replicable across various wings/branches/sections in the field audit offices. The material must provide for self-learning and continued learning even after the training. The training plan must include appropriate methodology to evaluate the trainees and measure the effectiveness of the training.

#	Training Type	Number of Trainees	Batch Size	Number of Batches	Number of Days per batch
1.	OIOS Application Phase 1 Training	420	20	21	5
2.	OIOS Application Phase 2 Training	420	20	21	5
3.	OIOS System Admin Training	45	15	3	3
4.	Designing of MIS reports / dashboards	420	20	21	3

13.3. UAT Training & Indicative Trainee Details

At various stages of the project (for every release), specialized UAT training should be provided to the various users who will conduct acceptance tests of OIOS System. The table below provides the training requirements.

S. No.	Training Type	Number of Trainees	Batch Size	Number of Batches	Number of Days
1.	UAT Training – Phase 1 (for two releases)	180	20	9	3
2.	UAT Training – Phase 2 (for four releases)	360	20	18	3

13.4. Indicative Training Coverage

The table below broadly illustrates the training type and the respective coverage from each training type.

#	Type of Training	Broad Coverage in Training
1.	Agile development methodology	SI to train the product owner's core team on the flavour of agile methodology to be used including concepts, terms and processes.
2.	Tool chain methodology	SI to train on the specific toolchain and using the same for defining and updating backlogs, updating statuses, watching progress of user stories, etc.
3.	Functional help desk tool training	SI to train functional help desk to add tickets, follow-up on tickets, escalate tickets and act as a co-ordinator between end-user community and technical help desk.
4.	UAT Training Phase 1 (For every quarterly release)	a) A thorough comparison study of the Phase 1 requirements vs the end product of Phase 1 OIOS system. b) Complete end to end basic walkthrough of all the modules of Phase 1 OIOS system.
5.	UAT Training Phase 2 (For every quarterly release)	a) A thorough comparison study of the Phase 2 requirements vs the end product of Phase 2 OIOS system. b) Complete end to end basic walkthrough of all the modules of Phase 2 OIOS system.

#	Type of Training	Broad Coverage in Training
Master Training Coverage		
6.	Application Training Phase 1 and Phase 2	The training should focus on the Master Trainer getting adequate coverage so they can train end users in their field audit offices to use the OIOS application: a) The Training shall be planned to cover role based and would focus based on every user category, including office and wing administration. b) The Training shall be planned to cover modules deployed in the respective phase. c) Training would cover basic knowledge on the application and its benefits. And also, it should cover specific use/working knowledge in depth of each module for the end user. d) This training should be in a role based, benchmarked and standardized format. It should also allow for self-learning and retraining. e) Training would include mechanism for demonstration using audio/video/simulated/demo practice exercises and evaluation.
7.	OIOS System administration training	a) The training will also cover administrative activities such as User Creation and maintenance, and creation of other master data for specific IA&AD offices. b) For Training on monitoring Application performance management, Security Components, EMS/ equivalent console, SLA monitoring and any other technical aspect for monitoring of OIOS System. c) The trainees will be selected by IA&AD based on relevant educational background, technical skill sets and also inclination towards technical roles.

13.5. Responsibilities of the selected bidder for training

The Selected Bidder shall be responsible for the following activities as part of the training:

a) Develop an overall training plan in consultation of the IA&AD.

b) Develop a Batch-Wise training schedule, curriculum, training material and methodology for evaluating the trainee and effectiveness of training.

c) Deliver training to nominated trainees while carrying out the training effectiveness evaluation.

d) All training material, documentation and end user manual would be provided by the SI.

13.6. Training Infrastructure and Location

Location: The location for both UAT Training as well as the End User Trainings would be at IA&AD Premise(s) at NCR – Delhi and other planned locations. IA&AD would bear the travel cost in case of locations other than NCR - Delhi. Upon mutual agreement, a part of the training may be conducted via video conference.

Training Infrastructure: The training facility would include the infrastructure required for conducting the training. It would include location/space for training, projector and laptop/ desktop for each participant which would be used during the training. This would be provided by the IA&AD.

13.7. Evaluation

Evaluation of trainee: The SI would propose suitable evaluation methodology (in consultation with product owner) for the following.

- Measure the understanding and capacity building of trainees.
- In case of the master trainers, the methodology with which the master trainers can evaluate their trainees must also be developed.

Evaluation of training: Training effectiveness would be measured primarily using feedback mechanism. For that, questionnaire would be designed accordingly by the SI and submit to IA&AD for approval. The questionnaire would be handed over to the participants after the training and they would rate the training effectiveness. The parameters and the scale for measurement would be mutually agreed between the product owner and SI. In case the average score of the training falls below expected level, then the training would be considered as ineffective and hence re-training has to be arranged by the Selected Bidder at no additional cost.

13.8. Online Help

In addition to the capacity building activities, the Selected Bidder shall be responsible to provide a detailed context-sensitive help material for all the possible actions and scenarios on all user interfaces in the OIOS System. The User Interface of the OIOS System will provide help facility which include:

i. Help Menu
ii. Help Buttons
iii. Help text
iv. Multimedia Learning Materials
v. E-learning
vi. Standard Operating Procedures
vii. User Manuals

Technical Response from the Bidder in Technical Format 12: The Bidder in the Technical Proposal should propose the

a) Approach, plan and proposed Training for conducting Training on UAT.
b) Strategy, approach, plan and proposed Trainers for conducting Training of Master Trainer both OIOS Application Phase 1, Phase 2 and Phase 3.
c) Strategy and approach for training on designing of MIS reports and dashboards.
d) Approach for evaluation and measurement of effectiveness of training.

14. Operations, Maintenance and Security Management Requirements

SI shall provide Operations and Maintenance (O&M) support for envisaged OIOS system for 7 years from the date of OIOS Application Phase 2 Go-live. The Operations, maintenance and security management requirements are detailed in the subsequent sections.

14.1. User Centralized Helpdesk Requirements

The operational support will have to be provided, through a suitable Helpdesk system, to ensure that the solution is functioning as intended and that all problems associated with operations are resolved satisfactorily. The selected bidder shall set up an appropriately staffed centralized helpdesk for providing helpdesk support to various users of the OIOS application. The helpdesk and its associated software and hardware components shall be deployed as required by IA&AD. IA&AD retains the right to request for onsite deployment, with 30 days' prior notice, which the SI shall comply.

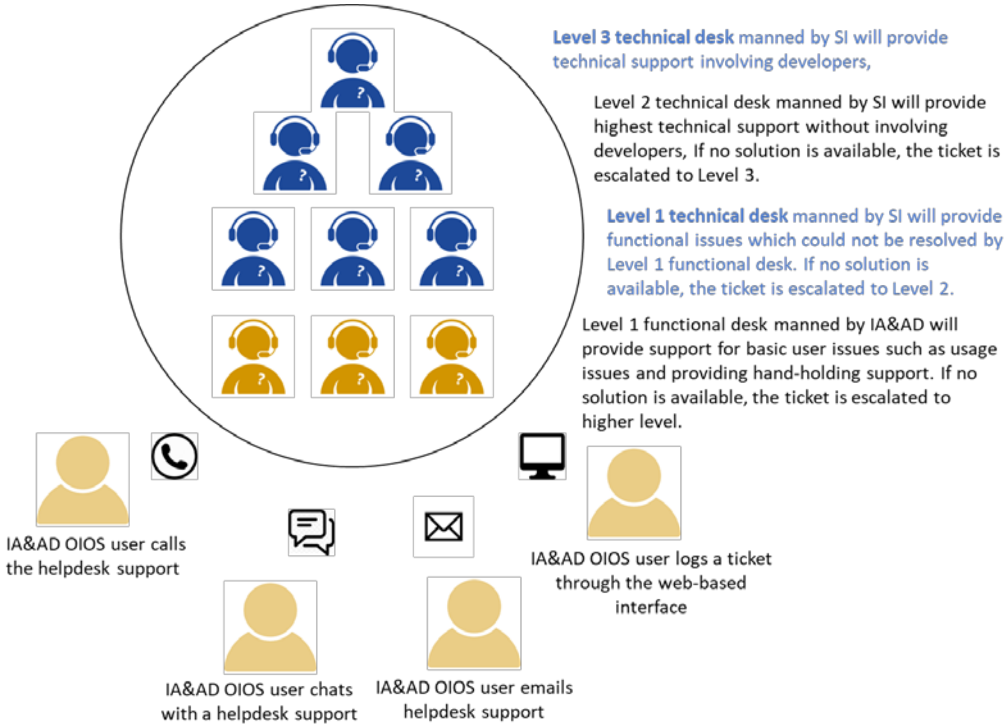
- The Centralized Helpdesk will serve as a single point of contact which shall be providing support on both technical and domain (business process) related assistance to IA&AD Users.
- The service will serve as a single point of contact for reporting / resolution of all tickets queries, errors, incidents, issues either business or application or infrastructure or operations.
- Troubleshooting Services including maintenance for overall system stabilization, defect resolution, system maintenance, system administration, availability & performance issues, security administration and database administration etc.
- Any User should be able to contact the Helpdesk through a (toll-free) number of 11 digits or by logging in a ticket in the application or Live chat or Email.
- A web-based application for service desk tool for registering the calls and a call logging system in line with the severity levels as per the SLAs shall be implemented within the OIOS system.

The levels of support provided through the centralised help desk is detailed below. All the levels detailed below will utilise the same platform.

- The first level of support is a **Level 1 functional help desk support**, which would be manned by IA&AD officials. They shall assist in hand-holding users and provide clarifications on usage issues.

If no solution could be provided by them, the ticket gets escalated to Level 1 technical support. They are trained to solve known problems and problems which are domain specific.

- The **Level 1 technical support** is manned by SI. These technicians are knowledgeable and experienced and will assist in resolving technical issues which could not be resolved by Level 1 functional support. The type of tickets would include issues relating to errors, incidents or operations. If no solution is available, the ticket gets escalated to Level 2 technical support.
- The **Level 2 technical support** is manned by SI. These technicians are highest technical resource available to resolve a technical issue without involving development. They handle incidents which could not be resolved by Level 2 technical support. If no solution is available, unless additional development is need to fix the issue, then the ticket gets escalated to Level 3 technical support.
- The **Level 3 technical support** is manned by SI. These technicians would handle incidents which could not be resolved by Level 2 technical support because it required development or code changes. It is important to note that these are bug fixes and not change management. The fix provided by Level 3 technical support may involve rolling out a patch for OIOS application.



Level 3 technical desk manned by SI will provide technical support involving developers,

Level 2 technical desk manned by SI will provide highest technical support without involving developers, If no solution is available, the ticket is escalated to Level 3.

Level 1 technical desk manned by SI will provide functional issues which could not be resolved by Level 1 functional desk. If no solution is available, the ticket is escalated to Level 2.

Level 1 functional desk manned by IA&AD will provide support for basic user issues such as usage issues and providing hand-holding support. If no solution is available, the ticket is escalated to higher level.

IA&AD OIOS user calls the helpdesk support
IA&AD OIOS user logs a ticket through the web-based interface
IA&AD OIOS user chats with a helpdesk support
IA&AD OIOS user emails helpdesk support

Figure 7: Centralized help desk

The core components of the user centralized help desk will have to be delivered using the SI's own resources; however, SI can consider using sub-contracting for part of this requirement as part of the overall Helpdesk delivery approach after prior approval of the IA&AD. Helpdesk tool shall be supplied and implemented by the selected bidder and provide for any hardware or software required for the same.

The broad set of activities as part of helpdesk support includes:

- Receiving incidents/requests through phone or email or web-app or live chat. Entering of the incidents in the helpdesk application and communicate the user of the unique incident id generated through email/phone/SMS. Selected bidder will be responsible for provisioning for converting these phone numbers into multiple lines as required.
- The helpdesk shall work during normal working hours of IA&AD.
- The Helpdesk service is required in English and Hindi language.
- Routing incidents internally between teams and tracking till resolution ensuring adherence to SLA. Providing updates to users on incidents logged.
- The SI in consultation with IA&AD is required to provide necessary channels for reporting issues to the help desk in OIOS application.
- Periodic reporting of incidents providing details including (but not limited to) number of incidents reported, reporting mechanism (phone/email/MIS).
- Creation of knowledge base on frequently asked questions (FAQ) to assist user in resolving basic issues themselves shall be ensured.

The SI will also submit an escalation matrix to IA&AD on the procedures for resolution of different types of issues/error/bugs and implement the same. Selected bidder should escalate any untoward incidents to IA&AD, on an immediate basis for reporting purposes / action from IA&AD. The selected bidder should also inform about the mitigation methods it has taken or proposes to take to resolve the issue.

SI shall deploy Helpdesk Resources in a time phased manner. Time phased Helpdesk resource requirements with team structure and skill set is provided in the table below. The requirements are indicative and may be augmented based on actual requirements arising with a prior notice of 30 days, which the SI shall comply.

S. No.	**Timeline**	**Yr1**	**Yr2**	**Yr3**	**Yr4**	**Yr5**	**Yr6**	**Yr7**
	Resource Category	**Qty**	**Qty**	**Qty**	**Qty**	**Qty**	**Qty**	**Qty**
1	Application Support Manager	1	1	1	1	1	1	1
2	Manager - L1 and L2	1	1	1	1	1	1	1
3	Analyst - L1	2	3	3	2	2	1	1
4	Analyst - L2	1	3	3	2	2	1	1
5	Analyst – L3	1	1	1	1	1	1	1
Year wise Resource Requirement		**6**	**9**	**9**	**7**	**7**	**5**	**5**

All resources should be minimum B. Tech / B.E/ MCA and have at least 3 years of work experience. The Manager position should have at least 5 years' experience.

Note: In this regard, it is once again stated that the selected bidder shall propose the resumes of the resources before operationalization of Centralized Desk to IA&AD or its nominated agency for approval.

14.2. Application Management

- SI shall be responsible for defect free operation of the envisaged system during the O&M period and ensuring its 24x7 availability at all the end-user locations and across all the channels of access. Any bugs reported in the application shall need to be fixed within a time frame mutually agreeable to IA&AD and SI.
- SI shall also be responsible for version control of the application files and shall need to update application documentation to reflect the current features and functionality of the application.
- SI shall provide a staging/ pre-production environment in the Primary Data Centre for testing of changes/ patches before applying them on production environment.

14.3. Infrastructure Management (PDC, DRC and Development Center)

Infrastructure management includes overall management and administration of entire IT infrastructure of all environments, PDC, and DRC at Tier-3 co-located DC/DR. SI shall be responsible for the following activities as part of infrastructure management:

- **Incident management**

- Provide resolution to incidents as per the resolution time limit agreed upon with IA&AD.

- **Problem management**
  - Perform root cause analysis for infrastructure problems/recurring incidents and initiate request for change.
  - Schedule and complete preventive maintenance activities.
- **Business continuity management**
  - Provide necessary support in ensuring business continuity.
  - Maintain asset register for all VMs, Platforms and software equipment.
  - Maintain a database of VMs count and configurations.
- **Change management**
  - Ensure that any component change due to any fault is replaced with a component of the same make and configuration.
  - Maintain records of all hardware, software installation, movement, upgrade, addition and change (IMAC) in the configuration database.
  - Perform impact analysis, create test plan, and develop rollback plans.
- **Availability management**
  - Review key monitoring parameters from availability point of view.
  - Performance tuning of the system to enhance system's performance and comply to SLAs on a continuous basis with no extra cost to IA&AD.
  - Provide prior communication on outages as per agreed communication processes.
- **Monitoring management**
  - Preparation of monthly dashboard on monitoring coverage, alerts generated/ closed, alerts escalated and other hits/ misses.
- **Backup management**
  - SI should evolve a backup and archival strategy.
  - Regular backups of project related data.

- Handling service requests on backup and restoration.
- Generation of monthly report on the backup/restoration performance.

- **Security management**
    - Real Time Security Threat Monitoring.
    - Reporting and resolution of security incidents.
    - Maintaining secure domain policies.
    - Escalation and co-ordination with other vendors for problem resolution.
- **Disaster recovery management**
    - Managing Disaster Recovery activities pertaining to Primary data center operations.
    - Conduct mock DR drills in a mutually agreed frequency or as per current Audit Criteria or its revision thereof.
- **General administration and support**
    - Providing suitable access to resources, designated by IA&AD, to tools being used monitoring infrastructure components.
    - Creation/deletion/modification of user accounts at the OS level.
    - Periodic review of user privileges at the OS level.
    - Password management.
    - Any other day-to-day administration and support activities required.
    - Clean up / archival of OIOS system logs operation.

14.4. Disaster Recovery Support

SI shall have complete responsibility in running the Disaster Recovery Center in case of failover of Primary Data Center. In addition, the SI is required to run Mock Drills once in six months.

14.5. Team for Operations & Maintenance of OIOS

1. The requirement of need for an onsite team for operations and maintenance of OIOS would be **decided by IA&AD based on the progress of the project three months** before completion of Phase 2, which SI shall comply.
2. Operation and Maintenance of the complete OIOS System and all associated system software and network for a period as specified in Scope of work post implementation of OIOS Application Phase 2.
3. Operation and Maintenance of the OIOS IT solution at Tier-3 co-located DC/DR and all associated system software and network for a period as specified in Scope of work.

An appropriately qualified, skilled and experienced team shall be deployed to perform the Operations and Maintenance responsibilities. The indicative Team size is as follows:

	Operations, Security and Maintenance Team: Indicative Team				
#	**Resource Type**	**Quantity**	**Duration in years**	**Min Qualification**	**Minimum Experience**
1.	Operations Manager	1	7	BE/B. Tech/MCA plus MBA	10 years
2.	Application Support	1	7	BE/B. Tech/MCA	7 years
3.	Developer/ Sr. Developer	2	7	BE/B. Tech/MCA	5 Years
4.	Tester	1	7	BE/B. Tech/MCA	5 Years
5.	DBA	2	7	BE/B. Tech/MCA	5 Years
6.	System Administrator	2	7	BE/B. Tech/MCA	5 Years
7.	Infrastructure Manager	1	7	BE/B. Tech/MCA	10 Years
8.	Analyst – BCP and Disaster Recovery	3	6	BE/B. Tech/MCA	10 Years
Security Administration Team					
9.	Security Manager	1	6	BE/B. Tech/MCA	10 Years
10.	Analyst (Application & Database Security)	3	6	BE/B. Tech/MCA	5 Years

14.6. Reporting Requirements

Phase	Report	Periodicity
Maintenance Phase	• Periodic update on maintenance activities • Periodic SLA performance reports	• As per SLA requirements/ as mutually agreed between IA&AD and SI

Technical Response from the Bidder in Technical Format 13 The Bidder in the Technical response should propose Operations, Security, Maintenance, SLA Management Roadmap and Reporting plan for all the project components to IA&AD.

15. Human resource deployment requirements

The selected bidder shall deploy project delivery team of suitably qualified and experienced managerial and technical resources for the successful development and rollout of OIOS System. The envisioned OIOS project shall be developed in a phased and staggered manner.

It is made clear that the entire team should be mandatorily deployed onsite at IA&AD **provided** premises at Delhi-NCR for project delivery at least up to the stage of **Phase 1 Stage 1 UAT**. The need for continued requirement for onsite deployment would be reviewed at least 30 days before end of **Phase 1 Stage 1 UAT** depending on the progress of the project, thus far.

The Development Center shall be provided by IA&AD and would be equipped with required furniture and internet facilities. The Onsite team should bring their end user computing device (Laptop/ Desktop) with all the necessary development and end point security software required for development of OIOS System.

15.1. Synopsis of Track-wise requirements

The table below provides an abridged requirement of OIOS project delivery requirements

Team Deployment Schedule for OIOS Project Delivery		
Phase	**Requirements**	**Duration**
Track 1	As required to fulfil requirements in Section 12	During the duration of development
Track 2	Dedicated Onsite (IA&AD premise at Delhi NCR) Resource Deployment for Development & testing of OIOS Application for Phase 1 Stage 1 UAT (at the minimum). The need for continued onsite presence, thereafter, will be reviewed at least 30 days before completion of phase 1 Stage 1 UAT based on status of implementation thus far. The same team will continue for the OIOS Application	As per Implementation timelines till **Phase 1** is successfully developed and implemented.

Team Deployment Schedule for OIOS Project Delivery		
Phase	**Requirements**	**Duration**
	Phase 2 and Phase 3. For further details, see subsequent sections.	
Track 3	As required to fulfil requirements in Section 12	During the duration of development, operation and maintenance Same as Track 1
Track 4	Onsite during the training schedule to fulfil requirements in Section 13	As and when training is scheduled.
Track 5	As specified in section 14.1. The onsite requirement of resources for help desk would be decided by IA&AD with a 30-day prior notice, which the selected bidder shall comply with.	Duration of 7 years from Phase -1 Go-Live
Track 6	As specified in section 14.5. The requirement of need for an onsite team for operations and maintenance of OIOS would be decided by IA&AD based on the progress of the project three months before completion of Phase 2, which SI shall comply	Duration of 7 years from Go-Live

15.2. Key personnel

The OIOS Project is a multi-disciplinary initiative with different phases and project tracks. This would require the Selected Bidder to deploy best in class resources having specialized skills, education and relevant experience for successfully implementing the project within time, meeting the scope and quality. The continuity of deployed resources in all the phases shall play a key role in meeting the project objectives. In the above context, the selected bidder should propose a **Team for Track 2: OIOS Application development of Phase 1, Phase 2 and Phase 3.**

The following points are stated in an objective manner:

- The selected bidder would propose the name and CVs of those lead members in the proposal who would be working in development and implementation of the OIOS System.
- Only these lead members who would be working in the OIOS System shall be present during the Technical Presentation during the Bid process.
- The SI would retain these lead members till the completion of OIOS Application Phase1, Phase 2 and Phase 3. These key resources should not be withdrawn from the OIOS Project, unless an explicit approval from IA&AD is sought for and received.

The requirements with regard to the key personnel are listed below.

S. No	Proposed Resource	Minimum Qualification	Minimum Experience	Full Time / On Demand (Remarks)
1.	Project Manager	BE/B.Tech /MCA and MBA	▪ Agile Certified Practitioner (ACP) from the Project Management Institute or equivalent ▪ Min 5 years of experience in executing Project in Agile Methodology ▪ Min 16 years of experience in IT industry	100% Full Time
2.	Scrum Master (one of the scrum masters will act as scrum of scrum).	BE / B. Tech /MCA and MBA	▪ At least one Agile Certified Practitioner (ACP) from the Project Management Institute or equivalent ▪ Certified Professional Scrum Master or equivalent	100% Full Time SI may choose to combine one of the scrum masters. But a minimum a two scrum masters must be provided.

S. No	Proposed Resource	Minimum Qualification	Minimum Experience	Full Time / On Demand (Remarks)
			▪ Min 5 years of experience in executing Project in Agile Methodology	
3.	Enterprise Solution Architect	BE/MCA	▪ 3 application implementation experience on the different business functions ▪ 16+ years of experience ▪ Should have industry standard certification such as TOGAF	25% Availability Onsite Available Onsite on Demand
4.	Business Analyst	BE/MCA + MBA	▪ 2 relevant application implementation experience ▪ 7 years of experience in relevant business function	100% Full time
5.	Database Administrator	BE / B. Tech / MCA	▪ More than or equal to 10 years' experience as a DBA	100% Full Time
6.	Security Architect	BE/B Tech/MCA	▪ Minimum 10 years of experience ▪ At least 3 large data center and enterprise security experience in Indian PSU/ Government Departments	50% Availability Onsite Available Onsite on Demand

S. No	Proposed Resource	Minimum Qualification	Minimum Experience	Full Time / On Demand (Remarks)
			▪ Conversant with ITIL, ISO 27001 standards ▪ At least one vendor neutral certification such as CISSP, CISA, CISM etc.	
7.	QC Expert	BE/MCA	▪ Experience in Functional Testing (Web, Mobile) ▪ Min 10 years of IT experience	100% Full Time.

Technical Response from the Bidder in Technical Format 8 and 8A: The Bidder in the Technical Proposal should propose the name of the Key Personnel in the Technical Bid Format 8 along with their role. The detailed CV of the Key Personnel should be provided in Format **8A.**

15.3. Track 2: Phase 1 and 2 Resource Deployment Requirement

The table below provides an indicative baseline resource category wise quantity, duration, minimum qualification and experience for the proposed development team.

Phase 1 and Phase 2: Indicative Team				
#	Resource Type	Quantity	Min Qualification	Minimum Experience
1.	***Project Manager***	1	***Provided in Key Personnel Section***	
2.	***Scrum Master***[7]	3		

[7] It may be also noted that one of the Scrum masters shall perform the role of Scrum of Scrum so as to maintain the consistency in approach across different Teams.

Phase 1 and Phase 2: Indicative Team				
#	**Resource Type**	**Quantity**	**Min Qualification**	**Minimum Experience**
3.	***Enterprise Solution Architect***	1		
4.	***Security Architect***	1		
5.	***QC Expert***	1		
6.	***Business Analyst***	3		
7.	Developers / Sr. Developers	15	BE/B. Tech/MCA	5 Years
8.	UX/ UI Designer	3	BE/B. Tech/MCA	5 Years
9.	Test Lead	1	BE/B. Tech/MCA	7 Years
10.	Testers	3	BE/B. Tech/MCA	5 Years
11.	Data Preparation / Migration Expert	1	BE/B. Tech/MCA	5 Years
12.	***Database Administrator***	1	***Provided in Key Personnel Section***	
13.	***System / Cloud Administrator***	1		

The table above depicting the team is indicative baseline only. The bidder is at liberty to augment the team composition and size over and above the baseline mentioned in above table whilst ensuring that the project timelines are met successfully. SI will not change the personnel deployed as Development team without due justification and prior approval of IA&AD. Change of personnel in the development team, shall be done only in case, if the personnel resigns from his/her organisation or due to medical incapacity; any such change in resource deployment shall be done only after the approval of IA&AD.

It is made clear, that IA&AD or its nominated agency reserves the option to insist SI to augment the Development Team for Track 2 - Phase 1 and Phase 2, with a three-week prior notice, which the selected bidder shall comply with.

It is again reiterated that the various teams deployed by the selected bidder shall bring their own end user computing devices. The end user computing devices (laptops / desktops) should have appropriate security solutions such as (Anti-Virus – Anti Malware etc.) to avoid security breach.

Technical Response from the Bidder in Technical Format 7, 7A and 7B: The Bidder in the Technical Proposal should propose the

a) Effort Estimate for Development of OIOS Phase 1 and Phase 2 Application.

b) Team composition with quantity for both Phase 1 and Phase 2.

c) Resource Deployment Plan as part of this Technical proposal for both Phase 1 and Phase 2.

(Premium, if any, for onsite deployment after Phase 1 may be mentioned only in the financial bid).

It is made clear that the roles of each category of resource should be clearly defined and it is also made clear that one category of resource cannot be used interchangeably for another role, except as specified in the tables above. Any other interchangeable use of resources (other than mentioned above) should be fully justified and require prior approval of the Product Owner.

15.4. Track 2: OIOS Phase 3: Resource Deployment Requirements

The team shall carry out the requirements gatherings for Phase 3 OIOS System in consultation with IA&AD. The outcome of the exercise would be the finalization of Phase 3 requirements. Upon approval of the Phase 3 OIOS requirements, the team shall propose an effort estimate, detailed project plan with deliverables and team composition for successfully developing the Phase 3 requirements for OIOS and implementing the system as per the Implementation and rollout plan. It is envisaged that the Phase 3 requirements aggregating 18 months of engagement may be split and provided to the SI in three packages of broadly 6 months each.

15.5. Mandatory Process before Deployment of Proposed Team

As a general principle, in any phase of the project, at the relevant stage the selected bidder shall propose the names of the resources for deployment. IA&AD or it’s nominated agency shall scrutinize the resumes and interact with the proposed resources before their deployment. After the express approval of IA&AD the resources shall be deployed.

In addition to the above, the performance of the deployed resources would be periodically assessed.

15.6. Performance Review of Team

The team members' performance shall be reviewed by IA&AD and its nominated agency on an ongoing, periodic basis. If IA&AD or its nominated agency finds the performance of one or more resources to be unsatisfactory, IA&AD shall have the option to ask for a replace with an adequately qualified and experienced replacement resource, with a three-week prior notice, which the selected bidder shall comply with.

16. Documentation Requirements

The Agreed and Final, Project Plan for both phases of OIOS must include a complete description of the proposed approach to the user and system documentation. All End-User documentations like end-user manuals, training materials and system operation and maintenance etc. should be in English.

The documentation relating to design and development should be maintained in the tool chain and other documentation should be maintained systematically in a document management system with appropriate version and configuration control.

User documents must be presented through the OIOS user interface and made available for download in acceptable formats such as Portable Document Format (pdf) and similar formats as needed. System Documentation is intended primarily for internal OIOS management team use and will not be made available through the portal.

Documentation must provide configuration management and document control information at the start of each version of the document. All documents should be provided to IA&AD in soft copy. The following are minimum documentation requirement in relation to OIOS project.

16.1. Design and development documentation

The documentation should be maintained as part of the tool chain.

- Product Backlog – User stories, priority, estimate of effort, Use Cases etc.
- Release backlog
- Minutes of release planning minutes.
- Preliminary Design Review document
- Sprint Planning document and its minutes
- Sprint Backlog
- Sprint metrics for monitoring progress
- Sprint Retrospective
- User Acceptance Report – Sprint review, Demo of Features, Definition of Done
- Issue Tracker and resolution of outstanding issues post Go-Live
- Test Plan & Test Reports

- Final OIOS documentation (to be given sprint wise) – Requirement specifications, Design (technical & functional), Code and Test

16.2. Documentation relating to training and capacity building

The user & training documentation shall provide complete and comprehensive user manuals that cover, but not limited to, the following aspects:

- Functional user manual (for application administrators, office administrators, wing administrators and other role-based users)
- How to training videos
- E-learning material
- Training documentation including material and evaluation
- Troubleshooting guide
- Quarterly Release Training documentation

16.3. Application system administration

The documentation relating to application system administration shall include, but not be limited to, the following:

- Installation
- Database Structure
- System Structure and control flow
- Interface to other systems
- Security control matrix
- Privacy control, integrity control, backup and recovery operation etc.

16.4. Documentation relating to operations, maintenance and security

The system operation and maintenance documents shall include, but not be limited to, the following:

- Equipment level operations
- System level operations
- Maintenance schedules and procedures

- Configuration Management Plan
- Troubleshooting including list of error messages
- Performance tuning and capacity planning
- Security administration
- Backup and recovery procedure

In addition, the security design document shall address following issues:

- Application security
- Database and Middleware security

16.5. Documentation relating to OEM/COTS/Open source components used

The documentation relating to OEM/COTS/Open source components used in IT solution shall cover, but not limited to, the following:

- IT Service management
- Management and Deployment of the software and standard software updates
- Management of the system's user move/add/change requests

Note: The document submitted to IA&AD should adhere to standards conforming to the best practices such as CMMI 5, ISO 27001, as applicable. These documents would be reviewed by IA&AD before final acceptance for its conformity with the relevant applicable standards.

17. Exit Management Plan and Handover Mechanism

The selected bidder shall prepare and provide the IA&AD a clear and unambiguous Exit Management Plan. Details of the Exit Management are furnished in volume-III of this RFP.

The Exit Management Plan shall contain the details thereof including the following:

(i) A detailed program of the transfer process that could be used in conjunction with IA&AD or the Replacement Vendor, including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure during the transfer;

(ii) Modalities for communication with SI's sub-contractors, staff, suppliers, service providers and any related third party as are necessary to avoid any detrimental impact on the Systems operations as a result of the transfer;

(iii) Plans for provision of contingent support to the project and IA&AD or the Replacement Vendor for a reasonable period after the transfer.

Handover Mechanism:

(i) At the end of the specified O&M services period, the IA&AD may exercise its option to renew the O&M services with the existing SI or decide to undertake these activities on its own or to a third-party

(ii) If Handover is required to IA&AD / any other vendor at the end of the existing O&M or otherwise, SI shall be responsible for handing over the complete know-how, documentation records, software logs and all such relevant items that may be necessary for the transition process

Technical Response from the Bidder in Technical Format 14: The Bidder in the Technical Proposal should propose clear Exit Management Plan and Handover Mechanism to ensure smooth transition.

18. OIOS Architecture

- The Solution Architecture comprising of Functional Architecture, Application Architecture, data Architecture, Technical Architecture and Security Architecture are provided in a separate document as a part of the RFP labelled as **Annexure B: OIOS Architecture to this document**
- The technical specifications for the various items are provided in a separate document as part of this RFP labeled as **Annexure C: IT Infrastructure and Technical components to this document.**

Technical Response from the Bidder in following formats.

- Format 9: Solution Proposed
- Format 9A: Software Architecture and Design to meet the Non-functional Requirements
- Format 9B: Sizing of Compute resources w.r.t to OIOS Phase 1 requirements including SLAs.
- Format 15 A: Proposed BoM/ Rate Card Matrix of the components for the Track 2: Middleware and Software requirements
- Format 15 A & B. Phase 1 & 2: Middleware and System Software
- Format 16: Specifications Card Matrix of the components for Track 3: Phase 1
- Format 16 A. Phase 1 at PDC: Hardware
- Format 16 B. Security at PDC
- Format 16 C. Setting up of Backup Site 1 and Lease Line Provisioning
- Format 17 & 17A: Requirement of the components, middleware and software for Phase 2
- Format 18: Requirements of the components for Track 3: DRC
- Format 18 A & B. Disaster Recovery Center: Hardware & System Software
- Format 18 C. Setting up of Backup Site 2 and Lease Line Provisioning

The Bidder in the Technical proposal should propose the overall solution, the architecture, the required hardware and software components to satisfy the requirements (functional, non-functional and others detailed in this RFP). The bidder is at liberty to add any extra item required for successful meeting of the requirements (including SLA) of IA&AD.

19. Non-Functional Requirements

The following are the non-functional requirements for the OIOS IT solution/project.

19.1. Performance

1. Performance is that aspect of service, which is measured in terms of throughput and latency. Higher throughput and lower latency values represent good performance of a service. Throughput represents the number of service requests served. Latency is the round-trip time between sending a request and receiving the response.
2. This test process will include the following activities:
    - Determination of performance metrics
    - Designing performance tests
    - Development of workload
    - Performance testing
    - Identification of bottlenecks and providing solutions
    - Determining final performance figures.
    - Communication of final results to all stakeholders
3. Final output of this process would be a sizing guide for the solution tested. The sizing guide will document the details of the performance tests, test data, bottlenecks identified, alternate solutions provided, and the final performance data.

The system should provide fast and steady response times (Quality of Service). The performance criteria are detailed in **'RFP Vol III, Annexure A: Service Level Agreement'**.

19.2. Availability

1. Availability of OIOS Application is a key requirement. The project must provide employees with timely, continuous access to information as per defined SLA. The project must also be able to

rebound or recover from any planned or unplanned system downtime, ensuring a minimal impact on the operations.

2. Availability is the quality aspect of whether the service is present or ready for immediate use. Availability represents the probability that a service is available. Larger values represent that the service is always ready to use while smaller values indicate unpredictability of whether the service will be available at a particular time.
3. Also associated with availability is time-to-repair (TTR). TTR represents the time it takes to repair a service that has failed. Ideally smaller values of TTR are desirable.
4. The availability test would include the following activities
    - Designing test for availability testing
    - Execution of availability tests
    - Assessment of transaction/data losses in relation to Disaster Recovery system
    - Communication of final results to all stakeholders

Note: Availability at all Web, App and Database server levels will be targeted. It is expected that selected bidder would maintain an average availability/uptime as mentioned in the SLA, of all components included but not restricted to hardware items, servers, database servers, system software, enterprise wide application software etc.

19.3. Security

1. Security is the aspect of the service of providing confidentiality and non-repudiation by authenticating the parties involved, encrypting messages, and providing access control. The applications can have different approaches and levels of providing security, depending on the service requester.
2. Security Process will include:
    - Audit of Network, Server and Application security mechanisms.
    - Assessment of authentication mechanism provided in the application/ components/ modules.

- Assessment of data encryption mechanism.
- Assessment of data access privileges, retention periods and archival mechanisms, etc.

3. Final outcome of this process would be a comprehensive audit report including all the Network, Server and Application security features incorporated in the OIOS Project.

For details refer to Annexure B and Annexure C. However, the following security requirements are the common, minimum requirements that will apply to the portal and all associated application systems:

I. The portal shall comply with a designated policy for the processes of secure data disposal from the system.

II. Sensitive data transmission and all administrative activities in the portal must be done in a secure channel (SSL).

III. Developers are expected to develop the portal security (SQL Injection, Cross Site Scripting etc.) while developing the web functionalities. Developer must adopt appropriate architecture and design guideline to avoid such web vulnerabilities.

IV. The portal should provide transparent and automated security management, security policy enforcement and automated password resets.

V. A range of web transactions will need to be secured in order that users' personal details are not exposed to inappropriate view. Where personal data is collected there shall be appropriate data protection notices provided to raise awareness on how that personal data will be processed. This shall be reinforced with an accessible Data Protection Policy Statement.

VI. The system shall meet Information Security Management requirements as detailed in ISO 27001.

VII. OIOS Application should be free from Top 10 OWASP 2017 or the latest revised vulnerabilities which can be found at < https://www.owasp.org/index.php/Top_10-2017_Top_10>

19.4. Usability

Usability is concerned with specifying the user interface and end-user interactions with the system. Usability incorporates well-structured user manual, explanatory error messages, help facilities and consistent interfaces enhance usability. The user interface must be very intuitive to facilitate easy on-boarding of first-time web application users.

The system should have the following flexibilities and functionalities in terms of usability:

- Comprehensive sitemap details in an easy to browse format.
- The system should ensure that same screen appears each time it is launched
- Consistent and logical navigation flow
- Usage of standard GUI features (E.g., pull-down menus, dialog boxes, toolbar buttons)
- Consistent look and feel
- The application windows colors must respond correctly to user changing of color settings (i.e., must change with the colors, or all must stay fixed).
- Data formats are consistent throughout application windows
- The menu options in the pages can be accessed via keyboard commands and/or arrow keys. Mouse-only access to options should be avoided.
- The system should ensure that controls on page must respond properly to Tab order and hot-keys (alt-keys).
- Provision for tool tips at each field and also online Help at the field level
- The system should prevent the users from errors and allow error recovery
- System should have user friendly submission guidelines for each form which is easily understandable by the user. For example, pop up for date should be “dd-mm-yyyy” and drop-down list for “fund code”, “return code” etc.

19.5. Scalability

The system should meet the following scalability requirements:

- Support the deployment of additional modules at a later point in time with minimal downtime and loss of productivity.
- Support multi-tier architecture and should have the capability to integrate with external / third party components like Rules Engine, Functional Modules etc. which should not be point to point integration, but with well-defined interfaces for data integration using enterprise data model
- Ability to scale horizontally without redesign
  - Multiple similar hardware and mix of multiple hardware in a horizontal setup.
  - Scalability for external components (External components should not restrict scalability)
- Support message patterns and protocols supported - E.g. publish/ subscribe, synchronous/ asynchronous, push/ pull/ pool, topics/ queues.

19.6. Portability

The portability requirements may be provided as follows.

- The solution should support ease of migrating applications and databases from one platform or technology to another.
- No OEM specific functionality of RDBMs to be used, which may become obstacle in changing RDBMs at a later stage.
- The users at IA&AD/ IA&AD should be able to access the applications on the existing OS, browsers etc. or platforms of similar nature or family without any machine-dependent installations.
- The solution should also be compatible to platforms commonly available in mobile devices.

19.7. Manageability

Manageability needs to be a crucial aspect of an Enterprise Solution. SI has to ensure that the solution deployed has adequate monitoring and tracking features for measuring the utilization and availability of resources. This includes:

1. Remote monitoring of Status and Statistics of all high-level components
2. Management capability to start/ stop/ restart services and systems
3. Auto discovery of all components manageable
4. Auto discovery of all other system components
5. Ability to track changes in configuration of the system components to help track service
6. System disruptions

20. Project Management Requirements

OIOS Systems is a multi-discipline, multi-dimensional initiative. An effective Project Management Plan and commitment to adhere to it is a mandatory requirement. The selected bidder shall prepare a Project Management Plan for Development and Implementation for each respective Phase requirements and submit to IA&AD for review, feedback and acceptance. The project plan should include the resource, task and timelines for the entire duration for the respective phase for each of the project track.

The selected bidder must employ best practises in project management methodology to ensure that the OIOS Application, tracks and components are developed and implemented within the defined time period. A copy of the project management schedule shall be handed over to product owner to keep track of the progress of the project.

SI would be required to deploy a full time Project Manager for the entire duration of project and a dedicated project team to deliver the project. The project manager shall act as the single point of contact for IA&AD. The selected bidder is required to propose a project team for Phase 1, 2 OIOS Implementation as well as Operations & Maintenance phase of the OIOS System.

20.1. Project Monitoring and Status Reporting

The SI would be required to provide periodic reports on the project progress. The status reporting shall be suitably adopted as per agreement with the IA&AD. The formats of the reports would be finalized after commencement of the project. During interim period, SI would provide adhoc report as per need basis. The Project Manager would also be responsible for escalating all issues in a timely manner. The documents and the status reporting must be part of the toolchain as far as possible or through a systematic document management system. The exact list of plan and reports that are required by IA&AD would be finalised after selection of the flavour of the agile methodology that is decided to be used during the development.

The indicative list of project management plans is given below.

- Project Organization and Management Plan
- OIOS System Development Plan with milestones and timelines
- Delivery and Commissioning Plan

- Testing Plan and Methodology
- Training Plan, Methodology and Training Details
- Change Management Plan
- Any other relevant items related to the OIOS Systems Implementation

The SI should provide all the project monitoring reports requested by IA&AD to assist in OIOS Project Monitoring on a weekly/monthly or on a need basis.

- Tasks completed during the week
- Periodic Project progress vis-à-vis planned as per the Sprint review meetings
- Compliance of potential improvements in future plan/sprints as per the Sprint Reviews
- Report on adherence/deviation from accepted OIOS architecture and concomitant compute resources
- Cumulative deviations to date from schedule of progress on milestones as specified in the agreed and finalized Project Plan
- Pending actions items from previous reporting period
- Forecast for the next reporting period
- Risk Reporting and Mitigation steps
- Corrective actions to be taken to return to planned schedule of progress, if any
- Proposed revisions to planned schedule
- Interventions which the selected bidder expects to be made by the product owner
- Other issues and outstanding problems, and actions proposed to be taken
- Results of training

Technical Response from the Bidder in Technical Format 11 & 19: The Bidder in the Technical response shall propose a Project Delivery and Management Plan covering all the project tracks for successfully delivering OIOS project. Technical proposal should comprise of amongst others project team structure, key activities with timelines, Rollout Plan, UAT Plan, risks and mitigation plan, quality plan, communications plan etc. The Plan should be logically organized for OIOS Application Phase 1, Phase 2 and Phase 3.

21. Quality Control Requirements

The following quality control requirements are envisaged for OIOS project. The quality control requirements may be suitably adapted for the exact flavor of agile development technology that is decided to be used during the development.

21.1. Quality Control for development

The purpose of quality control is to identify defects/issues from the work products early in the life-cycle. Quality Control occurs throughout the development from the beginning with verification of the requirements, progressing through the verification of the evolving deliverables, and culminating in the verification of the completed product. The verification process should address whether the work product properly reflects the specified requirements. The validation demonstrates that the product/applications and deliverables, as provided, will fulfil its intended use. The end users and other relevant stakeholders are involved in the validation activities including requirements and design review by IA&AD and User Acceptance Test (UAT).

With respect to Quality Control activities, the selected bidder will propose standards and guidelines for Quality Control requirements. It includes but not restricted to code review, unit test, integration test, system test and Load testing. SI will undertake code reviews to ensure quality and to implement the standards and guidelines, selected bidder will plan for peer review and test activities in detail. Coding standard needs to be identified and followed by selected bidder during development phase. Selected bidder will prepare required test scenarios and test cases to verify the functionalities as mentioned in requirements. Test defects needs to be captured, analysed, reported and closed. It is expected that selected bidder will develop a bi-directional Requirements Traceability Matrix (RTM).

To ensure timelines and quality, IA&AD envisaged solution delivery through iterations in OIOS Application development using Agile/Scrum methodology (or any other flavour prescribed by SI in consultation with product owner). The criteria for acceptance will be defined by the product owner.

The review of IA&AD would include a UAT, code review and documentation review. Hence, the selected bidder should prepare user manual for the sprint and impart UAT training for every release. The code review and documentation review shall be undertaken by the product owner’s team or his/her nominated agency. SI shall propose use of an automated toolchain to carry out testing at different stages.

21.2. Test Documentation

Test Plan/Review Plan:

The scope of the test activities, the methods and tools, the schedule and sequence of all test activities related to the OIOS have to be stated and defined in this plan. The test objects have to be identified as well as the attributes which have to be tested and the related end of test criteria must be fixed. Responsibilities and risks have to be identified and documented.

Test Case:

In the test case specification, the test object has to be identified as well as the attributes which have to be tested. It has to be made clear which steps and measures have to be applied to execute the test cases and which results are expected.

Test Data:

The test data to execute the test cases would be provided by IA&AD.

Test Result:

The test results have to be documented and it has to be identified if the test ended with the expected results i.e. if they passed or failed. The test recording strongly depends on the test environment. In some cases, this can be an automatic printout. In other cases, this may be a check list which is ticked by the tester (may be even included in the test procedure / test case specific). It may be even necessary to apply different methods within the same project, depending on the kind of test object and the kind of test employed. A preparation of the test results in a report is required. Test logs may be voluminous and have to be condensed to have their contents prepared for a quick overview and reference as well as for management or customer presentations.

21.3. Defect Management Guidelines

The defect management process involves documenting, tracking, resolving and closing issues or defects in the test environment. The process defined within this section highlights how defects will be prioritized and assigned to responsible parties for analysis.

A defect can be identified when:

- A test case fails (actual results differ from expected results).
- A code deployment, configuration, or data issue is discovered during test environment verification.
- A connectivity, security, or work-station related issue is discovered that prevents test case execution.

The Test Team will examine and classify each identified defect by the severity of the problem and fix the same.

22. Adherence to Standards, Policies and Guidelines

The requirements relating to adherence to standards, policies and guidelines are detailed below.

22.1. Portal Design Guidelines

1. The system should support Unicode UTF-8 encoding facility.
2. All the forms / screens should be in English. However, all scheduled languages should be supported in word processing, data elements and documents stored in document management system.
3. Support multiple dates and time formats (especially dd-mm-yyyy which is the most prevalent in India). The user on the web portal should be able to change the date format as required.
4. The portal must comply with guidelines as specified by Government of India and available at www.web.guidelines.gov.in
5. Documents may be stored in the portal document repository using many formats, such as Word, Excel, Pdf etc. It should also have the capability to convert documents to other desired format. The portal must maintain the capability to read all the formats of all the documents that it manages, or has links to, irrespective of the age and version of the original native format of the document.
6. All data and applications delivered through the portal must be fully usable with all common web browsers, including at minimum Microsoft Internet Explorer, Safari, Chrome and Firefox.
7. No special client software shall be required to use any aspect of the data or applications delivered through the website.
8. The system must be "device aware" and vary content and access based on which device a user is utilizing i.e. users can securely access the portal via alternate devices, such as Tablet and mobile phones.

22.2. Conformance to Technology & Standards

During the implementation following standards & guidelines of MEITY would be referred/ used:

- The solutions would be made centralized, multi-tenant, integrable and support open APIs

- **The application would be built using preferably open source software and open standard platform and adhere to policies set out by MEITY on Open Source, Open APIs, Principle of e-Kranti, Software development and Reengineering guidelines.**
- The solution would leverage use of Controller of Certifying Agency empanelled agencies for authentication (Aadhaar based authentication and e-KYC using biometric devices), Digital-Locker, Digitize India, e-sign, PayGov India, National Payment Gateway platform, Mobile-Seva etc.
- The solution would be scalable and replicable with minimum changes, for similar kind of operations.

Interoperability is defined as the ability of two or more systems or components to exchange information and use the information that has been exchanged. Data standardization and interoperability are prerequisites for sharing and interfacing Department / Directorate systems/ Data with other National Agencies / State Agencies and businesses. To this end the Solution should be based on Open standards. Interoperability related projects should be compliant to CMIS standards for Content and Document management, HTTP/HTTPS/SOAP standards for SOA, BPEL 2.0 and BPMN 2.0 for Integration and Workflow. The Web portal should follow the GIGW guidelines.

The list of standards is indicated for reference but may not to be treated as exhaustive:

- Portal (Web pages) development W3C standards
- Information access / transfer protocol SOAP, HTTP/HTTPS
- Interoperability Web services open standards
- Digital Signature RSA standards
- Document Encryption PKCS specifications
- Secure Communication SSL protocol
- PDF 417 as 2D Bar Code standard
- Information Security ISO 27001 Standards
- 2-Factor RBAC Authentication and Authorization (user ID, password, and a digital certificate or
- Documentation IEEE/ ISO/ CMMi specification

22.3. Compliance to NeGP Framework

The solution architecture for the applications should be based on the layered architecture approach, allocated with a different set of service components like presentation, business, security, data access and data storage components. Each layer would be loosely coupled with the adjacent layers providing demarcation of functionalities. Components in each layer will interact with components of neighbouring layers only. The layered approach ensures a clean division of responsibility and makes the system more scalable, flexible, maintainable and extensible with a high level of cohesion between components. Proposed solution should be exposing the services in a Service Oriented Architecture (SOA)

22.4. Compliance with Open Standards

Open standards are of major importance for the success of all such ICT based governance projects in both the short- and long-term duration. By adopting open standards, the vendor lock-in and technology lock-in can be avoided. Open Standards provide standard interfaces and models for the data to be exchanged and are the key enablers for establishing well-functioning service-oriented architecture.

22.5. Compliance with Open Source Software Policy of GoI

- The solution would be made centralized, multi-tenant, integrable and support open APIs
- The application would be built on **open source software** and **open standard platform** and adhere to policies set out by Meity on Open Source, Open APIs, Principle of e-Kranti, Software development and Reengineering guidelines.
- The solution would leverage use of Controller of Certifying Agency empanelled agencies for authentication, Digital-Locker, Digitize India, e-sign, PayGov India, National Payment Gateway platform, Mobile-Seva etc.
- The solution would be scalable and replicable with minimum changes, for similar kind of operations

Note: The bidder has the liberty to propose proprietary software with a justification for adopting the same to meet the functional, technical and non-functional requirements. The bidder shall clearly state in the technical proposal why the same cannot be achieved using open source software. The justification will be assessed by IA&AD evaluation team.

22.6. Technology Standards

S No	Technology Standards
I.	**Architecture**- The application architecture should be n-tiered and must include all necessary software components. Architecture shall allow for future scalability and scope addition by way of defining new services.
II.	**Interoperability** - SI shall propose the solution and technology platform that is based on the open standards, provide interoperability with other operating systems and application servers, guarantee portability of data and content and that the best meets the functional, non-functional and technical specifications provided in the RFP. SI must follow the Deity guidelines on open standards available at http://egovstandards.gov.in/
III.	**Integration with Existing IT Applications**: SI should ensure that the proposed solutions are having necessary interfaces for data exchange with the existing IT applications.
IV.	**Web Services**- SI should ensure that the solutions proposed be integrated based on open standards supporting Web Services principles
V.	**Multilingual interface** - The system should provide multilingual interface/labels in languages of minimum English.
VI.	**Compatibility** -The system should run on multiple browsers
VII.	The solution architecture should be platform, database and vendor independent.
VIII.	The solution is required to provide modularity (business function and process) that should support addition / removal of one or more modules as and when required.
IX.	The solution should ensure data safety and integrity in the event of communication channels operation failures, software and hardware operability failures.
X.	The solution should have the ability to scale up as and when the new business applications and services are added without compromising the performance of the overall solution. The architecture should be proven to be highly scalable and capable of delivering high performance as and when the transaction volumes increase.
XI.	System should employ a common user access and authentication service to ensure Single-Sign on for the end-user.
XII.	The system should be developed to be deployed in n-tier data center Architecture.

S No	Technology Standards
XIII.	System should be extensible to provide access to the interfaces through mobile data terminals.
XIV.	System should support secure transmission of data over the network and support Secured Socket Layer (SSL).
XV.	Any access to the solution database shall only be via application after appropriate authentication
XVI.	System should support requirement of OTP and digital certificates for authentication and non-repudiation.
XVII.	As part of their Technical Bid Response, the SI shall provide the detailed architecture and comprehensive Bill of Materials/rate card matrix for all components of the proposed solution.
XVIII.	**Mobile App - Offline – Online Mode** The Mobile Application should work in both online and offline mode and have the capability to synchronize with the central application once the data generated in offline mode gets the required connectivity.

23. Definition of “Go Live”

The OIOS IT solution would be considered for “Go Live” after completion of development and roll-out of Phase 2. The completion of phase 1 (i.e. Phase 1 acceptance) is only considered as a “partial” Go Live (also termed as Phase 1 Go Live). The definition of “Go-Live” in deciding the date of completion of contract would be the “final” Go Live after completion of Phase 2, as defined in this section. It is important to understand the definition of “done” of a user story before the definition of “Go Live” of the OIOS project. The criteria for definition of done for each user story is defined by the product owner.

23.1. Definition of “Done” of a user story

a) The functional and non-functional tests that were defined within the scope of the user story have been conducted and passed;

b) All code has been reviewed;

c) All coding standards have been met and code has been re-factored where necessary;

d) Any necessary documentation has been completed and handed over to IA&AD;

e) All of the above have been accepted by the Product Owner.

23.2. The definition of “Go Live”

1. The OIOS Platform is considered Go-Live or “Go-Live” when the following are accomplished or delivered:

    a) All user stories in the updated product backlog, as agreed by the product owner, are “done”.

    b) The **resources have been commissioned at the Tier-3 co-located DC/DR** and integrated as per the RFP and are accepted by Product Owner.

    c) The **VAPT is completed** for modules released prior to Go-Live and accepted by the Product Owner.

    d) Completion of security audit by STQC or CERT-In empanelled vendor and the application reaches the status of “Safe-to-host”.

e) Product Owner in consultation with SI identify the issues which are critical for Go-Live. The issues which are not critical for Go-Live will be resolved during operation and maintenance phase.

f) All the **outstanding issues** are **identified** as **critical** to Go-Live issues are resolved

g) All the deliverables are delivered and are accepted by the Product Owner.

23.3. Process for acceptance of "Go-Live"

The Product Owner from the IA&AD and Project Manager, Scrum of scrum from SI will jointly initiate the notice for declaring "Go-Live" after satisfactory completion of all of the following.

a) All the activities as listed in Volume I of this RFP.

b) After scrutinizing all the deliverables, reports, audit findings, Contracts, licensing agreements etc.

1. The "Go-Live" notice is submitted to the Product Owner for action.
2. Within thirty days of receiving the notice, the Product Owner will decide on the actions to be taken on "Go-Live".
3. The Go-Live date comes into effect only when the Product Owner approves the notice for "Go-Live".
4. In the event that Product Owner does not approve or suggest further action, the notices are reinitiated only after the recommended actions have been satisfactorily completed.

Note: **Acceptance for OIOS shall be provided by Product owner and not individual offices.**

Comptroller and Auditor General of India

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Request for Proposal

`Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

'One IA&AD One System' (OIOS) Project

VOLUME – I – Annexure A

Reference Number: 51-ISW/2019-'One IA&AD One System' Project

Table of Contents

OIOS Functional Requirement Specifications

1 Introduction

The Comptroller and Auditor General of India (C&AG) discharges his constitutional functions through the Indian Audit and Accounts Department (IA&AD). It is the duty of the C&AG to audit the receipts and expenditure of the Union and each State and Union Territory Government, and such other entities as prescribed by or under laws made by Parliament. The Audit Reports of the Comptroller and Auditor General are placed before Parliament or the Legislature of the State or the Union Territory, as the case may be. More information about the C&AG and IA&AD is available at https://cag.gov.in/, in particular the Performance Report for 2017-18 at https://cag.gov.in/sites/default/files/performance_activity_report/PA_2018_1.pdf.

The 'One IA&AD One system' (OIOS) project aims at creating a single source of truth regarding audit activities of IA&AD. IA&AD has seen several IT applications that catered to the needs of one or more offices in this regard. OIOS will bring together the best practices of the various IT applications into one single enterprise-wide IT application. This IT application will be designed in such a way that it can be configured and used by any audit office in the IA&AD.

This document enumerates the functional requirement specifications of the IT solution envisaged as part of OIOS project.

1.1 Fundamental principles

The fundamental principles governing the design of OIOS IT solution are the following.

- OIOS will be the single source of truth regarding the envisaged activities within its scope.
- The activity or process itself must be captured in OIOS and hence avoiding post-facto data entry to the maximum possible extent.
- OIOS should aim to capture the common minimum / mandatory audit processes across various offices and provide scope for wing / office / audit-stream-wise configuration.

1.2 List of references

The following reference documents are available in the website of Comptroller & Auditor General of India (www.cag.gov.in) for further documentation.

- Organisational information (https://cag.gov.in/content/organisation-chart)
- Audit mandate
  - Constitutional provisions (https://cag.gov.in/content/constitutional-provisions)
  - C&AG's DPC Act, 1971 (https://cag.gov.in/content/duties-power-and-conditions-services-act)
  - Audit regulations (https://cag.gov.in/content/audit-regulations)
- Performance activity report (https://cag.gov.in/performance-activity-report)
- Auditing standards (https://cag.gov.in/content/cag%E2%80%99s-auditing-standards)
- Main auditing guidelines and Manuals

    - Financial Attest Audit Manual (https://cag.gov.in/sites/default/files/manuals/Financial_Attest_Audit_Manual.pdf)
    - Performance Audit Guidelines (https://cag.gov.in/sites/default/files/guidelines/PA_Guidelines2014.pdf)
    - Compliance Audit Guidelines (https://cag.gov.in/sites/default/files/guidelines/Compliance_Guidelines_approved_final_preface.pdf)
- Repository of Audit reports (https://cag.gov.in/audit-reports)

1.3 Modular approach

The business process of IA&AD is bundled into business modules[1] and each bundle/ business module is described in a separate document. It is important to note that the bundling only represents business process modularisation and does not reflect the modules of the IT application. This modularisation provides the flexibility to on-board specific field audit offices or parts of field audit offices or specific activities across offices. After briefly describing the set of processes in a module, each chapter also deals with actors/roles involved and indicative list of activities envisaged in the IT solution.

Each of these modules produce outputs which can be downloaded and printed. While being printed, these outputs[2] leave the traceable digital channel. OIOS IT solution should provide a means to verify the authenticity of the output. For this purpose, QR Code or similar machine-readable label may be considered to be part of the output so that the authenticity can be easily verified.

The high-level list of business modules along with their broad objectives envisaged in the OIOS system is detailed in the Table below.

Ref. No.	Business Module	Broad objectives
01	**Organisation**	• Maintain a master list of offices in IA&AD and their reporting hierarchy. • Maintain the internal structure of an office, including the posts and associated responsibilities. • Use the internal structure as a base for logical access control including formation of user groups, roles, privileges and workflow.
02	**Personnel**	• Maintain a master list of employees including their profile, recruitment, promotion, posting, transfer and nominations including training. • Interface with the Public Financial Management System (PFMS) (Employee Information System module), which is an IT application of the CGA. • Manage processes for leave, tour, employee claims etc.

[1] Modules relating to service books, annual performance appraisal, disciplinary proceedings, and integration with legal systems have been kept out of the scope currently. They may be included later at appropriate time frames, if felt necessary.

[2] Audit products, Audit observations, Audit enquiries, Audit requisition and any dispatch out of the 10: Communication module (say, audit intimation).

Ref. No.	Business Module	Broad objectives
03	**Auditee Universe**	• Maintain a master list of auditee entities under the mandate of C&AG[3]. • Maintain the allocation of auditee entities to offices/ wings/ branches in the organisational structure. This, along with the organisation structure, define the record-based permissions and workflows.
04	**Audit Planning**	• Prepare strategic audit plans[4] for IA&AD and each field audit office of IA&AD, along with documentation of the process. • Prepare annual audit plans for each field audit office and IA&AD (as well as rolling plans for the next two years), along with documentation of the risk-based preparation process. • Select the auditee entities for each of the audit assignments[5]. • Review progress against audit plans.
05	**Audit Design**	• Create the audit guidelines, including ◦ Creating the Audit Design Matrix, which includes design/ definition of audit objectives, sub-objectives, and questions, and ◦ Defining the sampling approach to be followed for each audit assignment, including selection of auditee entities and/or transactions. • Design and disseminate IT-based tool kits, as appropriate, for conducting the audit. This is handled in alignment with Business Module 09- Data Collection Platform
06	**Audit Execution**	• Intimation of forthcoming audit to auditee entity • Prepare **Audit Requisition** for records (paper-based/ electronic) and receipt of records. • (Optional) Prepare and communicate **Audit Enquiries**. • Finalise **Audit Observations** based on records and replies that were received. • Attach Key Documentary evidence (KDs) and other supporting documents. • Documentation of Entry and Exit Meetings/Conferences with Auditee Entity. • Receive records, responses to audit enquiries/ observations from auditable entity through digital interfaces (API Integration with external applications). This is handled in alignment with business module **'10 - Communication'.**
07	**Audit reporting**	• Prepare draft audit product(s) (E.g. Inspection Report, Statement of Facts, Draft Paragraphs, Departmental Appreciation Note, Management letter, C&AG's Audit Report

[3] Unstructured/semi-structured information about auditees will be maintained through Business Module 12 – Knowledge Management System.

[4] Presently, IA&AD does not consistently prepare Strategic audit plan.

[5] Selection of auditee entities for different audit assignments could take place either at the annual audit planning stage or the audit design stage.

Ref. No.	Business Module	Broad objectives
		and various forms of Audit certificates for financial attest audit). • Mark and link the Key Documentary evidence (KDs) in the draft. • Conduct QA/ QC of draft audit product at various levels (in Field Headquarters, C&AG’s Office) as appropriate for the type of draft audit product. • Prepare, review, approve, issue and receive responses to audit products • Add recommendations (as part of audit products). • Receive responses to draft audit products from auditable entity through a digital interface (API Integration with external applications). This is handled in alignment with b**usiness module ‘10 - Communication’.**
08	**Audit follow-up**	• Pursue[6] observations in selected audit products (E.g. Inspection Reports, Departmental Appreciation Notes, etc.) internally. • Maintain information regarding external follow-up mechanism (PAC/ CoPU) – including Department’s Explanatory Notes on findings in C&AG’s Audit Reports and Department’s Action Taken Reports on PAC/ COPU Recommendations. • Receive responses from auditable entities and follow-up on audit products through a digital interface (API Integration with external applications). This is handled in alignment with business module **‘10 - Communication’.** • Follow-up on action taken by auditable entities on recommendations of audit. This will be used to support follow-up audits.
09	**Data collection platform**	• Facilitate collection of data on an adhoc / assignment basis for a variety of purposes. Some illustrative purposes include returns from field audit offices to C&AG’s Offices; consolidation of returns by field Headquarters from various wings/ branches; beneficiary Surveys as part of Performance Audit Assignments; information/ feedback from external stakeholders on specific topics; IT-based audit toolkits etc. The activities related to data collection are listed below. • Design format for data collection. • Assign access to collect information. • Publish to begin collection. • Collect data. • Update formats for data collection. • Complete collection and consolidate data collected. • Maintaining a central repository of templates.

[6] Pursuance includes processing of responses of auditable entities and following up on action taken by the auditable entities on audit observations.

Ref. No.	Business Module	Broad objectives
10	**Communication**	• Maintain a DAK management system including, • Receive inward communication through paper-based letters, faxes, emails and digital interface (uploads from web-links, API interfaces with auditable entities, NIC's e-office DAK, etc.) – '**Receipt'** • Scanning of receipt (wherever applicable) • Transfer the receipt to wing/ branch/ section concerned for processing through a workflow. • Send outward communication through paper-based letters, faxes, emails and digital interface (API interfaces with auditable entities, NIC's e-office DAK, etc.) – '**Dispatch'**.
11	**ITA/PR/IW (Internal Test Audit, Peer Review, Inspection Wing)**	• **Plan and conduct Internal test audit**: Inspection/ internal audit (by a separate section within the Field audit office) of individual sections/ branches/ wings/ activities of a Field audit office. • Carry out peer review of field audit offices by nomination (by C&AG Office) of peer-level officials on an assignment-by-assignment basis. • Conduct (by C&AG Office) of inspection (internal audit) of a field audit office; including Inspection (by C&AG Office) of a set of field audit offices based on a theme. • Follow-up of findings and recommendations arising out of the above.
12	**Knowledge Management System (KMS)**	• Maintain documents and records relating to audit guidance. • Maintain documents (semi-structured/ unstructured) relating to auditee entities. • Maintain a central repository of audit design matrix, audit checklist and audit tool kits. • Maintain structured data (financial and transactional/ MIS) relating to auditee entities and perform data analytics and data service delivery (self-service and managed services). • Maintain a media repository. • Forum, wiki and instant messaging facilities.
13	**Reporting/BI**	• Provide a platform for self-serviced and managed services for MIS reporting and dashboards.
14	**Technical Guidance and Support (TGS)**	• Provide Technical Guidance and Support (TGS) for audit by Examiner/ Local Fund Accounts of Panchayati Raj Institutions (PRIs) and Urban Local Bodies (ULBs).
15	**Administration (non-HR)**	• Manage procurement process. • Maintain assets (movable and immovable) and inventory of the organisation. • Manage requests for information under the RTI Act and Complaints.
16	**Data migration**	• Migrate legacy data available across field audit offices.

1.4 Sub-modules in each business module

The business modules are further broken down into various sub-modules for ease of on-boarding on a modular basis. The sub-modules of each of the modules are listed along with their broad objectives in the following sections. To clarify, these sub-modules represent convenient grouping of business functions/ activities and NOT the specific sub-modules of the IT system to be developed. **One sub-module that is not envisaged as part of the RFP is elaborated in Appendix I to this Annexure. This is to ensure that the design of OIOS takes cognizance of the sub-module and its functionalities to ensure possibility of future integration.**

1.4.1 Organisation (01)

The sub-modules of Organisation Business Module are listed below.

01_Organisation		
Ref. No	**Sub-module**	**Broad objectives**
01_01	Office Master	Maintain list of offices/branch offices[7] and their reporting relationship.
01_02	Office Structure	Maintain the internal hierarchy in each office/branch office, which will form the basis for configurable workflow.
01_03	User Privileges Master	Maintain immutable (Department-wide) list of privileges relating to activities that can be done in OIOS.
01_04	User roles Master	Maintain a list of user roles which have a defined set of privileges / authorisations. Though a default set of user roles would be available, this sub-module is to be kept configurable for each field audit office. This is because the bundling of user roles might vary depending on human resources deployed and the office's structure (E.g. multiple roles could be grouped together for smaller field audit offices but could be divided in a highly granular fashion in very large field audit offices).
01_05	User role – Office structure mapping	Maintain the link between office structure and user role.

1.4.2 Personnel (02)

The sub-modules of Personnel Business Module are listed below.

[7] Field Audit Offices also have Resident Audit Offices, but these will not be managed through the Office Master and will be managed as audit teams.

02_Personnel		
Ref. No	**Sub-module**	**Broad objectives**
02_01	Employee master	Maintain a master list of employees along with basic information.
02_02	Employee profile	Maintain basic profile information along with qualification details of the employee. Receive relevant data relating to employee, which is maintained in Employee Information System module of PFMS application.
02_03	Posting/Transfer[8]	Maintain data regarding posting of an employee to an office, then specific wings and posts in the office (original and additional charges). Maintain data relating to transfer of an employee from one post to another. Maintain data relating to posting of an employee for field assignment (within and across functional wings of FAO). **Note:** This module does not involve assigning employees to field audit assignments. Assigning employees to audit teams who will undertake audit assignments is handled in sub-module '**06_01: Audit programme**' in module '**06: Audit execution**'.
02_04	Gradation list	Maintain data relating to promotion. Facilitate preparation and annual update of the "Gradation List" of employees (by cadre/ grade by the cadre controlling authority).
02_05	Training nomination	Manage master list of training courses offered by various training organisations (internal to the Department and external) along with documents. Manage training nominations of an employee, details of training attended, exemptions from training. Provide for a platform to upload related documentation regarding the same.
02_06	Other nominations	Maintain information regarding nominations, exemptions from nominations. Provide a platform to upload documentation regarding the same.
02_07	Leave	Manage the leave application and approval process of an employee.
02_08	Tour	Manage the tour programme processing of an employee. This includes the programmes of employees posted in the field.
02_09	Personnel Claim management	Manage the processes of application, review and approval process for claims (Travel, Medical, LTC, other allowances, etc.) by employees. This does not include payment processing by PFMS. However, an API interface with PFMS may be envisaged in future.

1.4.3 Auditee universe (03)

The sub-modules of Auditee Universe Business module are listed below.

[8] The purpose of this module is NOT to document the basis for posting/ transfer. Instead, the allocation/ assignment of employees to a particular position will be the basis for mapping of user roles in OIOS.

03_Auditee_Universe		
Ref. No	**Sub-module**	**Broad objectives**
03_01	Auditee Universe master and allocation[9]	Maintain the basic information about auditee entities along with hierarchy. Maintain the jurisdiction of each field audit office providing a mapping between auditee entities and the field audit office/ wing/ branch. This mapping also forms the base for record-based permissions.
03_02	Auditee Universe profile	Maintain profile information for auditee entities with configurable additional fields. Any other semi/ unstructured additional information or structured data may be kept as part of the auditee information system in sub-module '**12_02: Auditee information system**' under business module '**12 -Knowledge Management System**'.

1.4.4 Audit planning (04)

The sub-modules of Audit Planning Business module are listed below.

04_Audit_Planning		
Ref. No	**Sub-module**	**Broad objectives**
04_01	Strategic audit plan (Currently not prepared)	Provide a platform to create, approve, amend, review progress of the strategic audit plan for IA&AD and field audit offices along with necessary documentation.
04_02	Annual audit plan	Provide a platform to create, approve, amend and review progress of the annual audit plan for a year and rolling plan for the subsequent two years for IA&AD and field audit offices along with necessary documentation. Select the auditee entities for the assignments forming part of the annual audit plan[10].
04_03	Audit risk (parametric)	Provide a platform to conduct quantitative risk assessment based on risk parameters (weighted risk score); both the parameters and the weights associated with each parameter should be configurable. Other kinds of risk assessment are currently kept outside the scope of OIOS. However, the documentation may be part of the Audit Planning and Audit Guidelines modules.

1.4.5 Audit Design (05)

The sub-modules of Audit Design module are listed below.

[9] The allocation of auditee entities to the jurisdiction of a particular field audit office does NOT prevent them for being covered in an audit assignment of another field audit office (e.g. District Collector offices will be audited by multiple State AGs).

[10] Selection of auditee entities for different audit assignments could take place either at the annual audit planning stage or the audit design stage.

05_Audit_Design		
Ref. No	**Sub-module**	**Broad objectives**
05_01	Audit design matrix	Select the auditee entities for the audit assignment. Provide a platform to layout audit objectives, sub-objectives (multiple hierarchical levels possible), audit questions[11] and prepare the audit design matrix. Provide a platform to link auditee entities to one or more levels. Provide a platform to attach audit toolkits at any level (objective, sub-objective, audit question)
05_02	Sampling approach	Define the sampling approach to be followed for selection of auditee entities and/or transactions.
05_03	Audit guidelines	Provide a platform to prepare, link relevant annexures and receive approval for audit guidelines. The link includes link to Audit design matrix from sub-module 05_01 and Sampling approach from sub-module 05_02.
05_04	Statistical sampling	Provide a platform to perform various types of sampling (E.g. simple random sampling – with/ without replacement, stratified random sampling, cluster sampling/multi-stage sampling and probability proportionate to size sampling.

1.4.6 Audit Execution (06)

The sub-modules of Audit execution module are listed below.

06_Audit_Execution		
Ref. No	**Sub-module**	**Broad objectives**
06_01	Audit Programme	Manage allocation of personnel to field audit programmes and its approval and deviation process. Communicate intimation of the program to the auditee entity.
06_02	Audit Requisition	Manage the process of requesting and receiving records (paper-based/ electronic) that are required for audit; also, the issue of reminders/ clarifications in case of non-receipt/ partial or incomplete receipt of records. It also monitors non-receipt and delay in receipt of records.
06_03	Audit enquiry (Optional)	Provide a platform to prepare, issue audit enquiry and receive reply to audit enquiry.
06_04	Audit observation	Provide a platform to prepare, issue audit observation and receive reply to the observation. The platform should have features to include text etc. from Audit Enquiries and replies to Audit Enquiries.
06_05	Audit toolkit (Collect) platform	Provide a platform to collect data in the field audit using audit tool kit that may be necessary for answering an audit question or fulfilling audit objective / sub-objective.

[11] The audit sub-objectives and questions may be applicable to all auditee entities and transactions covered in the audit assignment or may be applicable to specific entities/ transactions (to be defined and configured).

06_Audit_Execution		
Ref. No	**Sub-module**	**Broad objectives**
06_06	API Integration	Provide a platform (using Business Module '10 – Communication') to integrate with external applications to send AR, AE, AO and receive response.
06_07	Offline utility	Provide a solution for accessing the OIOS application when the employees are in places where there is unreliable or no internet connectivity. This may be envisaged as part of a mobile application. Provide a mobile application for scanning of the key documents.

1.4.7 Audit reporting (07)

The sub-modules under Audit reporting module are listed below.

07_Audit_Reporting		
Ref. No	**Sub-module**	**Broad objectives**
07_01	Audit product configuration	Provide a platform to create a new audit product type or amend audit product type, define common fields to be maintained across IA&AD. Provide a platform to configure additional fields to be maintained by the field audit office and/or its functional wings within the field audit office and configure modified workflow applicable to the field audit office and/or its functional wings. Configure the workflow for the audit product (depending on audit product type). This may involve workflow (often in an iterative manner[12]) within the functional wing of FAO, to the Head of the Field Audit Office, or to C&AG's Office.
07_02	Drafting Audit Product	Provide a platform to prepare a draft Audit Product, fill the necessary fields and link the key documentary evidence in the content. The platform should have features for including text etc. from Audit Observations, and replies to Audit Observations. The platform should also have the ability to include templates for the format of the Draft Audit Product, including auto-generation of the entire product or parts of the product.
07_03	Quality Control/ Quality Assurance	Provide a platform to verify the quality of submitted observations on validity and adequacy of audit evidence, and compliance with process parameters, within a field audit office or functional wing of FAO.
07_04	Finalisation and issue of audit product	Provide a platform to support finalisation of audit products submitted by the field audit offices by C&AG HQ. Provide a platform to review the content of the audit product, work collaboratively and finalise the audit product (iterative process). Issue the audit product after finalisation to the auditable entity.

[12] Not all of the iterations will be captured through workflow. Many of these iterations, especially within the Field Audit Office, take place based on face to face discussions.

07_Audit_Reporting		
Ref. No	**Sub-module**	**Broad objectives**
07_05	Receive response to draft audit product	Provide a platform to receive response to the draft audit product, process the response and, if necessary, send a rejoinder back to the auditable entity.
07_06	Recommendations	Provide a platform to maintain audit recommendations.
07_07	API Integration	Provide a platform to issue products / draft products to auditable entities, receive responses etc. via API interface (using Business Module '**10 – Communication**').

1.4.8 Audit follow-up (08)

The sub-modules of Audit follow-up are listed below.

08_Audit_follow-up		
Ref. No	**Sub-module**	**Broad objectives**
08_01	IR/ DAN/ ML follow-up	Receive reply to observations which were issued through Audit Products other than the C&AG's Audit Reports (Inspection Report/ Departmental Appreciation Note/ Management Letter[13], process the reply and send a rejoinder[14]. Implement a workflow (configurable by audit product type and other criteria) for closure/ settlement of observations featured in Audit Products. Provide a platform for documenting meetings (Apex Committee Meetings/ Audit Committee Meetings/ Joint Sittings) for discussing and settling audit observations covering a group of audit products (e.g. by District/ State Government or Central Government Department).
08_02	PAC/ COPU/ PAC/ COPU/ Another Legislative Committee[15] follow-up	Provide a platform to implement PAC/ COPU/ Other Legislative Committee follow-up process of audit reports. This will involve the following broad steps: • Submission of Explanatory Notes (ENs)[16] (usually received through the PAC/ COPU Secretariat) by State/ Central Government Departments on the individual findings included in the C&AG's Audit Reports; and vetting/ comments of the ENs by the concerned Field Audit Office to the PAC/ COPU Secretariat, and an iterative process thereon. • Correspondence (unstructured) between the Field Audit Office and the PAC/ COPU Secretariat on the selection of audit

[13] To the extent that the findings in the DAN/ ML are followed up independently, and not through the Inspection Report

[14] A response from IA&AD to the reply of auditable entity is referred to as 'rejoinder'.

[15] Public Accounts Committee (PAC) and Committee on Public Undertakings (COPU) are Committees of Parliament/ State Legislature to whom the C&AG's Audit Reports stand referred (as per Parliamentary/ Legislative Rules) after being tabled in Parliament/ Legislature.

[16] In differing auditee jurisdictions, this may be termed as "Detailed Explanation" or "Action Taken Note"

08_Audit_follow-up		
Ref. No	**Sub-module**	**Broad objectives**
		observations for oral examination of the Departmental Secretary by the PAC/ COPU - Preparation of a draft “Memorandum of Important Points (MIP)[17] on observations selected for oral consideration, for the PAC/ COPU Secretariat. - Submission of action taken reports by Central/ State Government Reports (routed through PAC/ COPU Secretariat) on the recommendations of the PAC/ COPU, and vetting comments of the Field Audit Office to the PAC/ COPU Secretariat, and an iterative process thereon.
08_03	API Integration	Provide a platform to integrate with auditable entities via API interface to receive response from the auditable entities (using Business Module **‘10 – Communication’**).
08_04	Recommendation follow-up	Follow-up on action taken by auditable entities on recommendations of audit.

1.4.9 Data collection platform (09)

The sub-modules of Data collection platform Business Module are listed below.

09_Data_Collection		
Ref. No	**Sub-module**	**Broad objectives**
09_01	Design data collection kit	Provide a platform to design the format of the data that is to be collected, and then publish the data collection format (including notifications through OIOS workflow, as well as e-mails to external participants, if necessary).
09_02	Allocate access	Provide a platform to allocate access by directly allocating to users or user groups or field audit offices for specific audit assignments.
09_03	Monitor data collection	Provide a platform to monitor the progress of data collection.
09_04	Consolidate and analyse data	Provide a platform to view consolidated data upon completion of data collection and perform basic analysis.

1.4.10 Communication (10)

The sub-modules of the Communication Business Module are listed below.

10_Communication		
Ref. No	**Sub-module**	**Broad objectives**
10_01	Receipt	Provide a platform to receive communication from outside OIOS (from outside and within IA&AD) in various formats – paper-based communication; fax; e-mail; interfacing external systems etc. into OIOS and allocate responsibility (through a configurable mechanism) for processing the communication.

[17] In differing auditee jurisdictions

10_Communication		
Ref. No	**Sub-module**	**Broad objectives**
10_02	Dispatch	Provide a platform to send communication outside OIOS (internally within an office, to other field audit offices or branch offices within IA&AD or to entities that are outside IA&AD) in various forms – paper-based communication; fax; e-mail; interfacing external systems and monitor the progress of action taken on the communication.
10_03	Notification and Alerts	Provide a platform for generation of notifications and alerts (configurable on various actions/ events within OIOS) through e-mail to staff within IA&AD as well as outsiders.

1.4.11 ITA/PR/IW – Internal Test Audit/ Peer Review/ Inspection Wing (11)

The sub-modules for internal control module are listed below.

11_ITA/PR/IW		
Ref. No	**Sub-module**	**Broad objectives**
11_01	Internal test audit	Provide a platform to plan and execute internal audit of wings/branches/sections within a field audit office, issue and follow-up of internal test audit observations.
11_02	Peer review	Provide a platform to plan and execute peer reviews of a field audit office, with a mechanism for follow-up by the concerned functional wing of C&AG Office.
11_03	Inspection wing	Provide a platform to plan and execute Inspections by the Inspection Wing in C&AG headquarters, with a mechanism for follow-up by the Inspection Wing and/or the concerned functional wing of C&AG Office. The wing also undertakes inspection assignments where multiple field audit offices are inspected based on a theme.

1.4.12 Knowledge Management System (12)

The sub-modules of the knowledge management system are listed below.

12_Knowledge_Management_System		
Ref. No	**Sub-module**	**Broad objectives**
12_01	Audit Guidance	Provide a platform for maintaining documents and records relating to audit guidance hierarchy (covering audit guidance issued by C&AG Headquarters Office as well as audit guidance issued by Field Audit Offices) with version control.
12_02	Auditee IS	Provide a platform for maintaining semi-structured/ unstructured documents relating to auditable entities with metadata tagging (and with role-based access control), and also features for review and archiving of documents, when no longer needed.
12_03	Central repository of audit design	Maintain a repository of audit checklists and audit toolkits (with categorization/ metadata tagging) for refinement and reuse by Field Audit Offices for future audit assignments.

12_Knowledge_Management_System		
Ref. No	**Sub-module**	**Broad objectives**
	matrix, check list and tool kits	
12_04	Auditee data warehouse/data analytics **(NOT IN SCOPE)**	Provide a platform to maintain structured data relating to auditable entities. For example, Accounting information in VLC, financial information in IFMS/PFMS/Treasury accounting systems, transactional and/or MIS data (Vahan/Sarathi, NREGA Soft, NSAP etc.) and make it available for users of OIOS. Also provide features for role-based access control. To provide self-serviced or managed service delivery for data analytics.
12_05	Forum	Provide a platform for informal group discussions based on subject matter of discussion, where instant response is not expected.
12_06	Wiki	Provide a platform to share audit experience informally.
12_07	Media repository	Provide a platform to maintain and forward/ circulate news digest manually and for advance web crawling/scraping/RSS feeds to create a media repository.
12_08	Instant messaging	Provide a platform for formal internal group discussions where instant/near instant response is expected.

1.4.13 Reporting/BI (13)

The sub-modules of Reporting module are listed below.

13_Reporting		
Ref. No	**Sub-module**	**Broad objectives**
13_01	MIS reports	Provide a platform to create self-serviced (and managed service) MIS reports as well as distributed MIS reports with parameters for managing/ controlling IA&AD audit processes.
13_02	Dash boards	Provide a platform to create self-serviced (and managed service) dashboards for managing/ controlling IA&AD audit processes

1.4.14 Technical Guidance & Support for audit by Examiner/ LFA of PRIs and ULBs (14)

14_Technical_Guidance_Support		
Ref. No	**Sub-module**	**Broad objectives**
14_01	TGS	Provide a platform for Technical Guidance and Support (TGS) of Audit by Examiner, Local Funds of Panchayati Raj Institutions (PRIs) and Urban Local Bodies (ULBs)[18]

[18] The primary responsibility for audit of the accounts of Urban Local Bodies (ULBs) and Panchayati Raj Institutions (PRIs) is usually vested by the State Government with the Examiner, Local Fund Audit or equivalent designation. The role of the C&AG and the field audit offices of IA&AD is to provide technical guidance and support (where entrusted by the State Government) to such audit by the Examiner/ LFA, as detailed in Chapter 10 of the Regulations on Audit and Accounts, 2007 (https://cag.gov.in/content/regulations-audit-accounts-2007#chapter10). Normal audit of ULBs and PRIs, where covered elsewhere under the C&AG's audit mandate, will be covered under the normal Audit Planning, Audit Execution, and Audit Reporting etc. Business Modules.

14_02	LB Committee of Legislature	Provide a platform to implement Legislative LB Committee follow-up process of LB audit reports, similar to the process followed by PAC/ COPU for other Audit Reports.

1.4.15 Administration – non-HR related (15)

The sub-modules of Administration Business Module (excluding the HR-related activities which are covered- in Business Module 02- Personnel) are listed below.

15_Administration		
Ref. No	**Sub-module**	**Broad objectives**
15_01	Office procurement	Manage procurement processes of an office.
15_02	Asset management	Manage information relating to assets (movable and immovable) of an office.
15_03	Inventory management	Manage inventory relating to consumables of an office.
15_04	RTI	Manage process of receipt and response to applications received under the Right to Information Act, 2005.
15_05	Complaints	Manage process of receipt and response to complaints received at various offices.

-

1.4.16 Legacy data (16)

The sub-modules of solution architecture requirements are listed below. The identified sub-modules are essential for the OIOS system but may be separate from the application that is developed by the System Integrator. The SI would be consulted before finalising the solutions.

16_Data migration platform		
Ref. No	**Sub-module**	**Broad objectives**
16_01	Bulk data migration service	Provide a platform for requesting bulk data migration service by uploading data in Excel file and attachments in zip file.
16_02	Ad-hoc data migration	Provide a platform to do data entry through prescribed web forms with the facility to upload attachments.

1.5 Roadmap: Release planning of sub-modules

The road map for modules of OIOS is drawn out in this section. The road map includes information regarding the time frame (shaded cells), coverage of field audit offices (colour of the shaded cells) and indicative release/bundle (number or alphabet within the cell) of business modules/sub-modules of OIOS. The entire project is divided into three phases. The requirements for sub-modules under phase 1 and 2 have been drawn out with reasonably sufficient detail. However, the requirements for sub-modules under phase 3 have been drawn at a broad level. It is proposed to follow an agile methodology for the product development in all phases.

1.5.1 Time frame

The time frame information includes time planned to taken for release/bundle planning, agile development (sprints including sprint planning, development, and review) and acceptance of design and development through user acceptance testing.

1.5.2 Coverage of field audit offices of IA&AD

In respect of phase 1 and phase 2, the sub-modules would be implemented in incremental coverage in three stages (after adequate testing) as detailed below. However, in respect of phase 3, the implementation of sub-modules would be an all-India level after adequate testing.

Stage 1: Development & Proof of core functionality: The sub-module functionality is envisaged to be developed and implemented in a few selected field audit offices (four to five) with an objective to validate the design at a basic level. The purpose is to validate the core functionality. This is the first stage of acceptance. This is denoted by **blue** colour.

Stage 2: Proof of ability to configure: The sub-module is envisaged to be implemented in the selected 31 pilot offices (excluding offices already covered in the proof of concept) and their respective functional wings in C&AG HQ covering a variety of audit streams. The objective of pilot implementation is to validate the applicability of the design across audit streams and validate the configurability features. This is the second stage of acceptance. This is denoted by **orange** colour.

The feedback received during testing of stage 1 and stage 2 would be considered ‘within scope’ of the RFP. That is, Additional story points or changes in story points that are added based on feedback received in stages 1 and 2 would **NOT** be considered as ‘**change management**’.

Stage 3: All-India implementation: The sub-module is envisaged to be implemented in all field audit offices and the sub-module reaches an irreversible status. At this stage, only configuration (and not change management/ customization) is expected, since the validation of configurability features has already been confirmed in the pilot implementation. This is denoted by **green** colour. Any changes required based on the feedback received during stage 3 (for sub-modules covered under phases 1 and 2) would be handled as a ‘**change management**’.

Phase 3: Any sub-module which will form part of future Time & Material phases but is part of the overall vision is denoted by **grey** colour. There would only be one stage of acceptance. The high level (not detailed) requirements of the business modules/sub-modules have been enumerated.

1.5.3 Phasing of development and implementation

Phase 1 and 2: The sub-modules to be developed and implemented in phase 1 and 2 have been divided into **eight** (indicative) releases. The releases are indicated with numbers in the cells of the table. Further, the road map also includes the extent of coverage in IA&AD, as detailed below.

Phase 3: The sub-modules to be developed and implemented in phase 3 have been bundled into three bundles (A, B and C). The bundle number has been indicated against the sub-modules to be developed in phase 3.

The complete information discussed above is illustrated in the infographic below. The sub-modules marked with ** would undergo modification until completion of phase 3. One sub-module (Auditee data warehouse) which would be handled independently is highlighted in black.

For the purposes of measuring completion, the last working day of the concerned quarter, as specified in the High-Level implementation timeline, is deemed to be the Project milestone for the relevant milestone for the purpose of this RFP, including the Service Level Agreement. This is applicable for Phases I and II only.

Table 1: Timelines for stage-wise implementation of sub-modules of OIOS (Road map)

	Phase 1		Phase 2				Phase 3 (T&M)						>>
Year	2020				2021				2022				>>
Quarter	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	>>
01: Organisation													>>
01_01: Office Master	1	2	3	4	5								>>
01_02: Office structure	1	2	3	4	5								>>
01_03: Privilege master**	1	2	3	4	5								>>
01_04: User roles	1	2	3	4	5								>>
01_05: Role-structure map	1	2	3	4	5								>>
02: Personnel													>>
02_01: Employee master	1	2	3	4	5								>>
02_02: Employee profile				4	5	6	7						>>
02_03: Posting/Transfer	1	2	3	4	5								>>
02_04: Gradation list		2	3	4	5								>>
02_05: Training					5	6	7	8					>>
02_06: Other nominations					5	6	7	8					>>
02_07: Leave									B	B			>>
02_08: Tour									B	B			>>
02_09: Personnel claim									B	B			>>
03: Auditee Universe													>>
03_01: Universe master	1	2	3	4	5								>>
03_02: Universe profile			3	4	5	6	7						>>
04: Audit planning													>>
04_01: Strategic Audit plan							A	A					>>
04_02: Annual Audit plan		2	3	4	5	6							>>
04_03: Parametric risk					5	6	7	8					>>
05: Audit Design													>>
05_01: Audit Design Matrix		2	3	4	5	6							>>
05_02: Sampling approach		2	3	4	5	6							>>
05_03: Audit guidelines		2	3	4	5	6							>>
05_04: Statistical sampling							A	A					>>
06: Audit execution													>>
06_01: Programme		2	3	4	5	6							>>
06_02: Record requisition		2	3	4	5	6							>>
06_03: Audit enquiry		2	3	4	5	6							>>
06_04: Audit observation		2	3	4	5	6							>>
06_05: TK-collect platform	1	2	3	4	5	6							>>
06_06: API Integration									B	B			>>
06_07: Offline utility			3	4	5	6	7						>>
07: Audit reporting													>>
07_01: Product configuration		2	3	4	5	6	7						>>
07_02: Drafting audit product		2	3	4	5	6	7						>>
07_03: QA/QC			3	4	5	6	7						>>
07_04: Finalisation & issue			3	4	5	6	7						>>
07_05: Receive response				4	5	6	7	8					>>
07_06: Recommendations					5	6	7	8					>>

	Phase 1		Phase 2				Phase 3 (T&M)						>>
Year	2020				2021				2022				>>
Quarter	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	>>
07_07: API Integration									B	B			>>
08: Audit follow-up													>>
08_01: IR follow-up				4	5	6	7	8					>>
08_02: LC follow-up				4	5	6	7	8					>>
08_03: API Integration									B	B			>>
08_04: Reco follow-up					5	6	7	8					
09: Data collection platform													>>
09_01: Design kit	1	2	3	4	5								>>
09_02: Allocate access	1	2	3	4	5								>>
09_03: Monitor collection	1	2	3	4	5								>>
09_04: Consolidate & Analyse	1	2	3	4	5								>>
10: Communication													>>
10_01: Receipt			3	4	5	6	7						>>
10_02: Dispatch			3	4	5	6	7						>>
10_03: Notification / Alert			3	4	5	6	7						>>
11: ITA/PR/IW													>>
11_01: Internal test audit											C	C	>>
11_02: Peer review											C	C	>>
11_03: Inspection wing											C	C	>>
12: KMS													>>
12_01: Audit guidance	1	2	3	4	5								>>
12_02: Auditee IS	1	2	3	4	5								>>
12_03: Repository of ADM/TK					5	6	7	8					>>
12_04: Data warehouse/data analytics	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	>>
12_05: Forum					5	6	7						>>
12_06: Wiki					5	6	7						>>
12_07: Media repository					5	6	7						>>
12_08: Instant messaging							A	A					>>
13: Reporting/BI													>>
13_01: MIS reports**		2	3	4	5	6	7	8					>>
13_02: Dashboards**		2	3	4	5	6	7	8					>>
14: Technical Guidance & Support													>>
14_01: TGS									B	B			>>
14_02: LB Committee									B	B			>>
15: Administration													>>
15_01: Procurement											C	C	>>
15_02: Asset											C	C	>>
15_03: Inventory											C	C	>>
15_04: RTI							A	A					>>
15_05: Complaints							A	A					>>
16: Legacy data													>>
16_01: Bulk data migration			3	4	5	6	7	8					>>

	Phase 1		Phase 2				Phase 3 (T&M)						>>
Year	2020				2021				2022				>>
Quarter	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	>>
16_02: Adhoc data entry			3	4	5	6	7	8					>>

01-Organisation Module

The organisation module in OIOS will assist in maintaining a master list of offices in IA&AD and their reporting hierarchy. It would also aid in maintaining the internal structure of an office including the posts and associated responsibilities. The internal structure of an office in IA&AD is the communication channel for flow of information and hence, the workflow. This module would also act to enforce logical access control viz., privileges, roles and role-structure mapping. The sub-modules in relation to the module are Office Master, Office Structure Master, User Privileges Master, User roles Master and User role – Office structure mapping.

1.6 Activities envisaged in OIOS

Configuring Organisation Master shall be the first activity of the OIOS Application, before other modules can be used. The activities (indicative) envisaged in OIOS have been listed below. However, the deliberations of task forces/committees/senior management meetings etc. along with the actual process of seeking approval of the competent authority for formation of offices/branch offices would be outside the OIOS ecosystem.

- Issue of order for formation of a new office/branch office.
- Issue of order for closure of an office/branch office.
- Modification of details relating to an office/branch office.

1.6.1 Issue of order for formation of an office/branch office

The standard operating procedure in the To-be process for formation of offices/branch offices is detailed below.

Process	**Issue of order for formation of a new office or branch office**	
Process trigger	Approval of competent authority to open a new office or branch office (Outside OIOS).	
Process Inputs	Documentation of approval of competent authority	
Process Outputs*	Communication of order to relevant stakeholders regarding formation of offices/branch offices. Push notification to C&AG website to update data.	
Actors involved in the Business Process	**Actor**	**Function**
	Application administrator	1. Create the new office (OIOS creates unique Office code) 2. Enter basic details 3. Assign reporting channel for an office?? 4. Enter Sanctioned strength of the office for different cadres, if available 5. Nominate office administrator, if known (This may also be done as a separate activity later). 6. Upload and link attachments such as documentation of approval of competent authority, deliberations/minutes of meeting/committees regarding the formation of office.
	OIOS System	1. **Master Data Management**: Acts as single source of truth for all IA&AD Applications.

Process	Issue of order for formation of a new office or branch office	
		2. Generate alert for all concerned, whenever change is made 3. Maintain change history
	Service Delivery Channel: OIOS	
System Interfaces with Other Modules/ Sub Modules/ External Stakeholders	Open API based access for all IA&AD Applications including C&AG website	

1.6.2 Issue of order for closure of an office/branch office

The standard operating procedure in the To-be process for closure of offices/branch offices is detailed below.

Process	Issue of order for closure of an office or branch office	
Process trigger	Approval of competent authority to close an office or branch office (Outside OIOS).	
Process Inputs	Documentation of approval of competent authority	
Process Outputs	Communication of order to relevant stakeholders regarding closure of offices/branch offices. Push notification to C&AG website to update data.	
Actors involved in the Business Process	**Actor**	**Function**
	Application administrator	1. Sets the status of the office as 'Closed'. (OIOS performs validation checks and prompts the user to enter effective date). 2. Upload and link attachments such as approval of competent authority regarding the closure of office.
	OIOS System	1. **Master Data Management**: Acts as single source of truth for all IA&AD Applications. 2. Generate alerts for all concerned, whenever change is made 3. Maintain change history
	Service Delivery Channel: OIOS	
System Interfaces with Other Modules/ Sub Modules/ External Stakeholders	Open API based access for all IA&AD Applications including C&AG website	

1.6.3 Modification of details relating to an office or a branch office

The standard operating procedure in the To-be process for modifying details relating to an office is detailed below.

Process	Modification of details relating to an office or branch office
Process trigger	Any event necessitating change of data elements relating to an office / branch office (Outside/Inside OIOS). For example, change of the head of

Process	**Modification of details relating to an office or branch office**	
	the office, change of location of office, contact information, reporting authority etc.,	
Process Inputs	Documentation of change	
Process Outputs	Communication of order to relevant stakeholders regarding modification of details relating to offices/branch offices. Push notification to C&AG website to update data.	
Actors involved in the Business Process	**Actor**	**Function**
	Office administrator	1. Make the necessary changes. 2. Upload and link attachments such as documentation of change.
	OIOS System	1. **Master Data Management**: Acts as single source of truth for all IA&AD Applications. 2. Generate alert for all concerned, whenever change is made 3. Maintain change history
	Service Delivery Channel: OIOS	
System Interfaces with Other Modules/ Sub Modules/ External Stakeholders	Open API based access for all IA&AD Applications including C&AG website and website of field audit offices	

2 Office Master (01_01)

The Indian Audit and Accounts Department (IA&AD) is headed by the Comptroller & Auditor General of India (C&AG). The Department is headquartered at New Delhi and has several field audit offices spread across the country falling under different categories and sub-categories:

- Audit Offices for the Union Government (Civil Audit, Defence Audit, P&T Audit, Railways Audit, Commercial Audit
- Audit Offices for State Governments
- Overseas and External Audit Offices
- Accounts & Entitlement (A&E) Offices[19]
- Training Institutes

The headquarters of IA&AD (C&AG HQ), also referred as the office of C&AG, has several wings. Some wings are responsible for administrative activities, while others are responsible for providing Quality Assurance/ QC for activities of field audit offices under their jurisdiction. Some field audit offices also have branch offices at various locations. The OIOS project presently envisages creating an IT based platform for the field audit offices and their branch offices.

The reporting structure of one office/branch-office to another plays a major role in determining workflow for finalising some of the audit products. Hence, it is important that OIOS should provide

[19] Not performing audit functions, not termed as Field Audit Offices, and not covered (except for limited scope) by OIOS

configurable features for capturing restructuring of offices, as and when implemented, while maintaining the history[20].

Further, OIOS should also provide for controlling visibility of data between offices. For example, a field audit office must have access to data of its branch offices as well.

The office master sub-module would assist in master data management of the field audit offices of IA&AD. The indicative business data to be maintained in office master is listed below.

Indicative business data for Office master
What are the field audit offices in IA&AD?
Does the field audit office have a branch office? If yes, which are the branch offices?
For each office/branch office, we will maintain the following in OIOS.

- Full name (The name varies based on the designation of the head of the office).
- Standard name (This is a more static name. Example Audit (Shimla), E&RSA (Gujarat)).
- Brief description of office
- GSTN#
- Audit stream (Lookup list - Central audit, State audit, Railway audit, Defence audit, etc.).
- Contact Address[21] – street address, city, state, Country, pin code
- STD phone number(s)
- PABX number(s)?
- Fax number(s)
- Email address of the office
- Reports to (The office to which it reports to)
- Date of formation of office
- Status of office (Open/Closed)
- Date of closure of office
- Designation-wise Sanctioned Strength[22]
- Documents relating to the office (Orders of formation, closure, etc.,)
- Details of whether the office is a cadre controlling authority? If yes, for which cadres of employees and which offices share this common cadre of employees?

2.1 Actors involved

The administrators at various levels would be responsible for creating the related information and keeping them up to date.

Application administrator (Central): When new offices or branch offices are created, the Indicative business data relating to the office or branch office is prepared by the application administrator. This

[20] Necessary features in the event of restructuring of offices (one-to-one; one-to-many; many-to-many) include (a) closure (but not deletion) of offices (b) re-mapping of employees as well as auditee entities from the old to the new offices (c) traceability, responsibility (for further processing, follow-up) and access to older audit products and supporting documentation between the offices and re-mapped auditee entities (d) mapping/ transfer of in-process workflows. These features will need to be implementable in the relevant business modules of OIOS. A similar approach will be needed for restructuring of the internal office structure of a field audit office.

[21] A few of the field audit offices are outside India.

[22] Not mandatory fields for filling in

actor is also responsible for migration of data from existing offices to the new offices. Depending on workload, this function could be split amongst multiple persons.

Office administrator: Once an office or branch office is created, an office administrator[23] would be nominated. The responsibility of upkeep of the information relating to the office / branch office will be that of the office administrator.

3 Office structure (01_02)

This sub-module would assist in capturing the internal structure of an office. Each Field Audit Office (FAO) has both headquarters (FAO HQ) and field audit teams. The FAO HQ consists of

- Wings headed by Group Officers, consisting of one or more branches
- Branches[24] headed by Branch Officers, consisting of one or more section
- Sections headed by Assistant Audit Officers/ Supervisors, consisting of one or more dealing hands and
- Dealing hands.

The field audit function of FAO includes both audit teams which permanently reside in auditee premises (Resident audit teams) and audit teams which are mobile moving from one audit assignment to another. This objective of the hierarchical structure (both in FAO HQ and the field audit teams) is to provide for segregation of duties and specialisation on specific set of activities. For example, a Planning branch including its sections and dealing hands would carry out activities that are related to preparation of audit plans.

The organisational structure of IA&AD, from an audit perspective, is depicted in the illustration below.

[23] We retain the possibility that the office administrator may be the administrator for the office and its branch offices also.

[24] Branch is NOT the same as a “branch office”. A branch is a part of a field audit office or a branch office, and not a separate office.

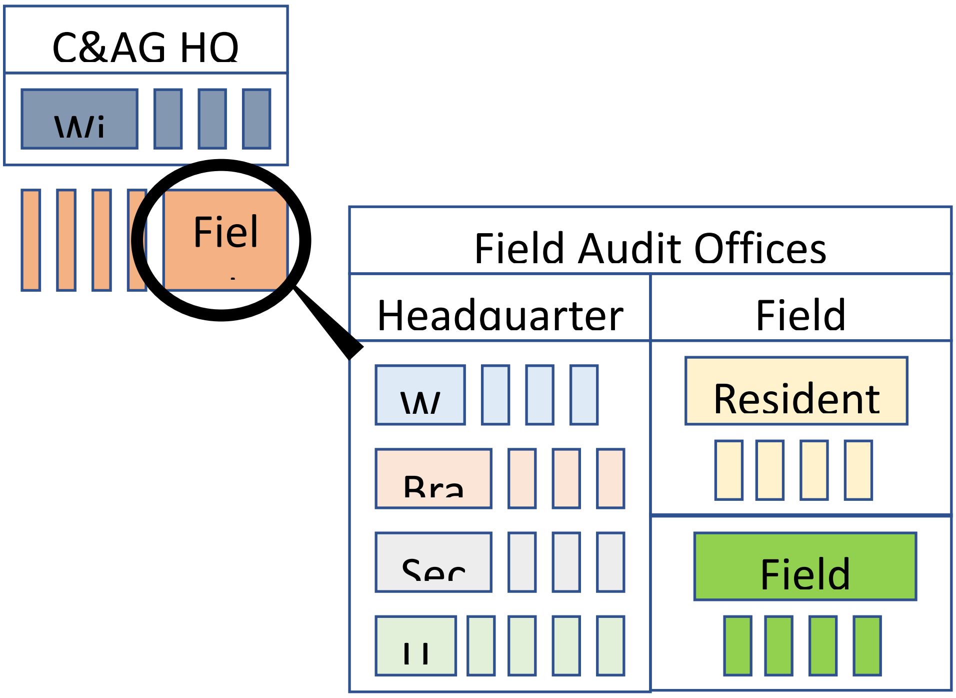


Figure 1 Organisational structure of IA&AD in the context of audit functions

The details of field audit offices and wings in C&AG HQ would be maintained as part of OIOS. The details regarding the master list of offices would be maintained by the application administrator in C&AG HQ. However, the organisational structure of an individual field audit office would be maintained by an administrator in the field audit office. The field audit office administrator will maintain the master list of branch offices under the field audit office. The organisational structure of a branch office would be maintained by the branch office administrator. The Indicative business data that are to be maintained for organisational structure is enumerated below.

Indicative business data for office structure master

Hierarchy – Office/ Branch Office → Wing → Branch → Section → Dealing hand;
Alternately, Wing → Resident Audit Team
What are the wings in each office / branch office?
What are the branches in each wing?
What are the sections in each branch?
What are the dealing hands in each section?
For each wing/branch/section/dealing hand, we will maintain the following in OIOS.

- Full name
- Standard name
- STD phone number(s)
- Status (Open/Closed)
- Date of creation
- Date of closure
- Documents (Orders of creation, closure etc.,)
- What are the duties and responsibilities of each wing, branch, section and dealing hand? This would form the basis for logical access control to determine user groups for separation of duties.

3.1 Actors involved

The administrators at various levels would be responsible for creating the related information and keeping them up to date.

Application administrator (Central): The office structure of C&AGHQ (Office of C&AG) will be maintained by the application administrator.

Office administrator: The office structure of the field audit office / branch office will be maintained by the office administrator.

Wing administrator: In the cases of large offices/branch offices, the office administrator may delegate the maintenance of wing-wise structure to the nominated wing administrators.

3.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS have been listed below. However, the deliberations of task forces/committees/senior management meetings etc. along with the actual process of seeking approval of the competent authority for formation of wings/branches/sections/dealing hands would be outside the OIOS ecosystem.

- Issue of orders for formation of new wing/branch/section/dealing hand in an office/branch office.
- Issue of orders for closure of a wing/branch/section/dealing hand in an office/branch office.
- Modification of details relating to a wing/branch/section/dealing hand.

3.2.1 Issue of order for formation of new wing/branch/section/dealing hand

The standard operating procedure in the To-be process for formation of offices/branch offices is detailed below.

Process	**Issue of orders for formation of a new wing/branch/section/dealing hand**	
Process trigger	Approval of competent authority to open a new office or branch office (Outside OIOS).	
Process Inputs	Documentation of approval of competent authority	
Process Outputs	Communication of order to relevant stakeholders regarding formation of the new wing/branch/section/dealing hand. Push notification to C&AG website to update data. Push notification to field audit office website to update data.	
Actors involved in the Business Process	**Actor**	**Functions**
	Office / Wing administrator	1. Create the new wing/branch/section/ (OIOS creates unique code) 2. Enter details 3. Assign reporting channel 4. Nominate wing administrator, if it is a new wing and if deemed necessary (This may also be done as a separate activity later). 5. Upload and link attachments such as approval of competent authority regarding the formation of the new wing/branch/section/dealing hand.

Process	**Issue of orders for formation of a new wing/branch/section/dealing hand**	
	OIOS System	1. **Master Data Management**: Acts as single source of truth for all IA&AD Applications. 2. Generate alert for all concerned, whenever change is made 3. Maintain change history
	Service Delivery Channel: OIOS	
System Interfaces with Other Modules/ Sub Modules/ External Stakeholders	Open API based access for all IA&AD Applications including C&AG website and field audit office websites.	

3.2.2 Issue of order for closure of a wing/branch/section/dealing hand

The standard operating procedure in the To-be process for closure of a wing/branch/section/dealing hand is detailed below.

Process	**Issue of orders for closure of a wing/branch/section/dealing hand in an office or branch office**	
Process trigger	Approval of competent authority to close a wing/branch/section/dealing hand (Outside OIOS).	
Process Inputs	Documentation of approval of competent authority	
Process Outputs	Communication of order to relevant stakeholders regarding closure of offices/branch offices. Push notification to C&AG website to update data (including closure/ re-referencing of sub-site of existing office)	
Actors involved in the Business Process	**Actor**	**Function**
	Office / wing administrator	1. Sets the status of the wing/branch/section/dealing hand as 'Closed'. (OIOS performs validation checks and prompts the user to enter effective date). 2. Upload and link attachments such as approval of competent authority regarding the closure of office.
	OIOS System	1. **Master Data Management**: Acts as single source of truth for all IA&AD Applications. 2. Generate alert for all concerned, whenever change is made 3. Maintain change history
	Service Delivery Channel: OIOS	
System Interfaces with Other Modules/ Sub Modules/ External Stakeholders	Open API based access for all IA&AD Applications including C&AG website and website of field audit offices	

3.2.3 Modification of details relating to a wing/branch/section/dealing hand

The standard operating procedure in the To-be process for modifying details relating to a wing/branch/section/dealing hand is detailed below.

<table>
<tr><th>Process</th><th colspan="2">Modification of details relating to a wing/branch/section/dealing hand</th></tr>
<tr><td><b>Process trigger</b></td><td colspan="2">Any event necessitating change of data elements relating to a wing/branch/section/dealing hand (Outside/Inside OIOS). For example, posting, change of contact information, reporting authority, access control etc.,</td></tr>
<tr><td><b>Process Inputs</b></td><td colspan="2">Documentation of change</td></tr>
<tr><td><b>Process Outputs</b></td><td colspan="2">Communication of order to relevant stakeholders regarding modification of details relating to offices/branch offices.
Push notification to C&AG website and/or field audit office website to update data, if necessary.</td></tr>
<tr><td rowspan="4"><b>Actors involved in the Business Process</b></td><td><b>Actor</b></td><td><b>Function</b></td></tr>
<tr><td>Office / wing administrator</td><td>1. Make the necessary changes.
2. Upload and link attachments such as documentation of change.</td></tr>
<tr><td>OIOS System</td><td>1. <b>Master Data Management</b>: Acts as single source of truth for all IA&AD Applications.
2. Generate alert for all concerned, whenever change is made
3. Maintain change history</td></tr>
<tr><td colspan="2"><b>Service Delivery Channel: OIOS</b></td></tr>
<tr><td><b>System Interfaces with Other Modules/ Sub Modules/ External Stakeholders</b></td><td colspan="2">Open API based access for all IA&AD Applications including C&AG website and website of field audit offices</td></tr>
</table>

4 User privileges master (01_03)

A field audit office has been structured internally to provide for segregation of duties. The structure also provides for specialisation of activities depending on availability of manpower. Thus, OIOS must include a functionality that helps in enforcing segregation of duties and specialisation, wherever necessary, through logical access controls. The first level of logical access control would be through user privileges or permissions. The user privileges for each module and the relevant sub-modules would be listed out during the Technical design phase. For example, View office structure, Add office, Modify office, Archive/Close office. This master list is immutable, i.e., it cannot be changed as any addition or modification would require change management in the application. However, administrators responsible for allocation of privileges would be able to view the same.

It is pertinent to note at this point that the permission may become further restricted based on record-based permissions. Let us consider the following example. Any office administrator will need the permission to edit phone number of an office. However, the office administrator cannot change phone number of any office other than the one he is nominated to. Hence, the privilege of ‘Edit office details:

Phone number' is to be restricted by record-based permission at an office level. Similarly, the ability to view details of branch offices or other offices reporting to an office may also be restricted through privileges.

Further, there might be branches in a functional wing of FAO which is restricted by record-based permission at various levels. Consider the illustration below and the Table which details the privilege of viewing auditable entities. While the branch Branch1 and Branch2 are restricted by record-based permission, the branch Branch3 is not restricted by record-based permission at branch level, i.e. the branch officer can view all auditable entities dealt by Branch1 and Branch2. However, the branch officer of Branch3 cannot view auditable entities of other wings.

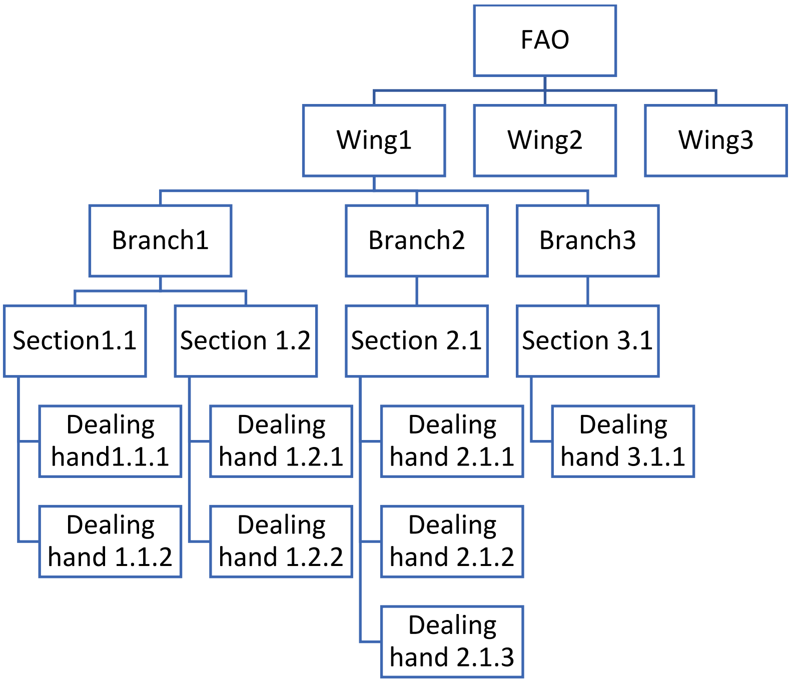


Figure 2: Illustration of office structure

Table 2: Record based permissions on privilege 'View auditable entities'

Structure	RBP level	Details
FAO	Office	Can exercise privilege on auditable entities related to office.
-Wing1	Wing	Can exercise privilege on auditable entities related to wing1.
--Branch1	Branch	Can exercise privilege on auditable entities allocated to section 1.1 and section 1.2.
---Section1.1	Section	Can exercise privilege on auditable entities allocated to dealing hand 1.1.1 and 1.1.2.
----Dealing hand 1.1.1	Dealing hand	Can exercise privilege on allocated auditable entities only.
----Dealing hand 1.1.2	Dealing hand	Can exercise privilege on allocated auditable entities only.
---Section1.2	Section	Can exercise privilege on auditable entities allocated to dealing hand 1.2.1 and 1.2.2.
----Dealing hand 1.2.1	Dealing hand	Can exercise privilege on allocated auditable entities only.
----Dealing hand 1.2.2	Dealing hand	Can exercise privilege on allocated auditable entities only.
--Branch2	Branch	Can exercise privilege on auditable entities allocated to section 2.1.

---Section 2.1	Section	Can exercise privilege on auditable entities allocated to dealing hand 2.1.1, 2.1.2 and 2.1.3.
----Dealing hand 2.1.1	Dealing hand	Can exercise privilege on allocated auditable entities only.
----Dealing hand 2.1.2	Dealing hand	Can exercise privilege on allocated auditable entities only.
----Dealing hand 2.1.3	Dealing hand	Can exercise privilege on allocated auditable entities only.
--Branch3	Wing	Can exercise privilege on auditable entities related to wing1.
---Section 3.1	Wing	Can exercise privilege on auditable entities related to wing1.
----Dealing hand 3.1.1	Wing	Can exercise privilege on auditable entities related to wing1.
-Wing2	Wing	Can exercise privilege on auditable entities related to wing2.
-Wing3	Wing	Can exercise privilege on auditable entities related to wing3.

Indicative business data for user privileges
Name of the module
Name of the sub-module
Privilege / permission
Is it restricted by record-based permission? If yes, at what level?

4.1 Activities envisaged in OIOS

The OIOS ecosystem will maintain the list of privileges so that it is visible for the administrator to allocate logical access to relevant employees.

5 User roles (01_04)

In order to facilitate easy allocation of privileges, the OIOS would facilitate group of user privileges or permissions into meaningful groups which would be referred to as ‘User roles’. This is the second step in configuring logical access control. For example, the user role ‘office administrator’ will be a group of all privileges or permissions that an ‘office administrator’ would have. The master list of user roles would be created and maintained by the ‘Application administrator’. It is pertinent that an analogy can be drawn between the actors in each of the process to roles.

Indicative business data in user role master
Name of the user role
Description of the user role
List of privileges grouped under a role

5.1 Actors involved

Application administrator: The app admin is responsible for creation and maintenance of user roles master. The administrator must be able to include or exclude user privileges from a user role, when necessary.

Office administrator: The office administrator must be able to view the user roles and the related user privileges. Though, the user role master at the application level should cater to most of the needs of the field audit office, there may be a necessity to create a role which is office specific. Hence, the office administrator would be responsible for creating office-specific roles wherever necessary, with notification to the application administrator. This feature must be used in a limited manner to avoid proliferation and duplication.

5.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS have been listed below. The activities would mostly be carried out during the initial deployments of the various modules of OIOS. After which, the changes are expected to be minimal.

- Create a new role.
- Include user privileges to a role.
- Exclude user privileges from a role.

6 User role-Office structure mapping (01_05)

As mentioned earlier, the internal structure of an office is normally a hierarchy with defined segregation of duties and specialisation at each level viz., wing, branch, section and dealing hands. An entity in a level is referred in general as a 'post' or a 'charge'. The mapping between a post/charge to a user role varies from one field audit office to another. A post/charge may be responsible for performing one or more roles. If a post/charge is mapped to more than one role, then, the post/charge would get a 'union' of privileges of all the roles allocated to it. Also, it is important to note that many posts could perform the same role, but with a different jurisdiction (e.g. different set of allocated auditable entities).

The assignment of an office employee to a post is envisaged through the Personnel Business Module.

For example, a planning section in a field audit office (named 'AAO/GEN' may be responsible for performing the roles of 'Plan preparer' and 'Programme preparer'.

Indicative business data in user role-office structure mapping
What are user roles for each charge/post?
What is the list of privileges that a particular charge/post gets based on the user roles allocated to the charge/post?

6.1 Actors involved

Application administrator: The application administrator is responsible for mapping of user roles with the office structure in the C&AG HQ.

Office administrator: The nominated office administrators are responsible for mapping of user roles with office structure in the respective field audit offices. They are also responsible for creating office-specific roles.

Wing administrator: In case of large offices/branch offices, the mapping of user roles with wing structure in the respective wings may be delegate to the nominated wing administrators by the office administrators.

6.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below. The activities would mostly be carried out during the initial deployments of the various modules of OIOS in an office. After which, the changes are expected to be minimal.

- Allocate one or more roles to a charge/post.
- De-allocate one or more roles to a charge/post.

02-Personnel

The personnel module of OIOS will aid in maintaining a master list of employees including their profile, posting, transfer, nominations for training / capacity building and other nominations relating to administrative activities[25]. This module will facilitate entry of relevant information as a post-facto activity (after obtaining approval of the competent authority) and be made available to the relevant stake holders. However, the communication of nomination to relevant stake holders and process of seeking exemption would be part of OIOS. This will ensure that the data relating to nominations will be up-to-date.

7 Employee master (02_01)

The master data relating to employees of IA&AD is envisaged to be maintained in OIOS. Each employee has a unique employee id and serves a particular designation at any point of time. The designations are hierarchical in nature. The processes of recruitment and promotions are very elaborate and vary for each designation and will be outside the scope of OIOS at present. The employee module may also be extended to A&E offices and Training Institutes in future. The minimum indicative business data that needs to be stored for each employee in the employee master is detailed below.

Indicative business data for employee master

- Unique employee id
- PFMS-EIS id
- Name of the employee (First Name, Middle Name, Last Name)
- Department assigned name (If there are two or more employees with the same name, the department assigns Roman numerals to differentiate them. For e.g. Manish Kumar – I, Manish Kumar – II, Manish Kumar – III).
- Type of employee (Permanent, Probationer, Temporary/Consultant, On-lien)
- Gender
- Batch of recruitment
- Category (General/SC/ST/ OBC)
- Handicapped category (Look up field)
- Date of birth
- PAN number
- PRAN number[26]
- AADHAR number
- Mother tongue
- Origin state
- Home town
- Permanent address
- Correspondence address
- Mode of recruitment
- Parent station

[25] The module does not aim to capture the working of the various committees/taskforces/wings involved in posting, transfer, assignments and nominations.

[26] For employees covered by the National Pension System (NPS)

- Parent office[27]
- Appointment Date
- Languages fluency
- AADHAR-linked Mobile Number
- Other Contact numbers
- NIC e-mail ID (used as the primary authentication mechanism in OIOS with mobile-based OTP; Two-factor authentication)
- Email ids
- Status of the employee (Working/Retired/Suspended/Under-probation)
- Present Grade/designation
- Is the employee presently on deputation?
- History of gradation list/designation changes and promotion
- Recent Photograph of the employee

7.1 Temporary resources

Some resources such as consultants, external experts, etc. would not be given an employee id since they are hired for a short term (Temporary resources). OIOS should provide a facility to register these users. These users would be provided temporary user id (temporary NIC e-mail ID) which expires on a date specified during the registration.

The same temporary registration sub-module can be used to facilitate temporary registration of staff of auditable entities during audit execution to facilitate communication of responses (e.g. to audit enquiries and audit observations). Alternative mechanisms for capturing such responses during execution of individual audit assignments may also be considered and proposed by the System Integrator (SI).

7.2 Actors involved

The responsibility of maintaining employee master level detail is with the application administrator and the employee.

Application administrator/Office administrator of the Cadre controlling authority: When an employee is newly recruited, the application administrator/OA of CCA is responsible for creating an entry for the employee (based on an intimation from the cadre controlling authority) and assigning an employee id[28] and entering basic details. A notification is issued to the employee upon creation of the basic details and subsequent modifications.

Employee: The employee would be able to change some of the basic details as and when it changes. For example, correspondence address, recent photograph, etc. Other changes to the basic details would require initiation and/or approvals by specifically authorized staff (e.g. change in hometown).

7.3 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Addition of details of an employee for the first time upon recruitment.
- Modification of details of the employee subsequently by office administrator.

[27] Not applicable for persons directly recruited into the Indian Audit & Accounts Services
[28] NIC e-mail id is currently assigned centrally.

    - Subsequent issue of notification to the employee after the change (System generated) which is validated by the employee.
- Modification of basic details of the employee subsequently by the employee (which may or may not require approval), or by specifically authorized users (depending on the data element).

8 Employee profile (02_02)

The information of employee regarding the qualifications, certifications and examination undertaken will be maintained as part of employee profile. The OIOS system will also maintain masters for the look up fields relating to the profile[29]. The employee must periodically review the profile information for updates/ continued accuracy and provide confirmation of the same.

Indicative business data relating to employee profile

- Educational qualification
    - Qualification (look up field)
    - Date of qualification
    - Institution
- Languages and associated level of proficiency, in particular knowledge of Hindi
- Professional certification
    - Certification (look up field)
    - Date of certification
    - Institution (look up field in the certification master)
- Examinations undertaken
    - Name of the examination
    - Dates of various papers in the examination
    - Status of various papers (Pass/Fail/Exempted/Did not attend)

Apart from the above indicative business data, the data of EIS module in PFMS needs to be studied to facilitate integration of PFMS data via API interfaces.

8.1 Actors involved

Office administrator: When an employee is newly recruited, the office administrator is responsible for entering details regarding the qualifications and certifications for the first time.

Administration wing: The administration wing is responsible for entering the details regarding application for writing the examination (conducted locally or centrally), papers in the examination, dates of examination and status relating to each paper. A notification is sent to the employee who then validates the data entered.

Employee: The employee would be able subsequently suggest changes and updates his profile regarding certifications and qualifications. This is added after approval by competent authority.

[29] The employee would also be allowed to suggest additions of other qualifications and certifications which are not in the master. This will be added to the master list after approval from competent authority.

8.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Addition of profile details by office administrator and employee.
- Modification of profile details by office administrator
  - Subsequent issue of notification to the employee, who validates the change.
- Suggest modification of profile details by the employee.
  - Subsequent approval by competent authority and notification to employee regarding approval.

9 Employee posting/transfer (02_03)

Each employee in IA&AD is given a specific role to perform a specific set of activities. This is referred to as a 'Post' or 'Charge'[30]. After allocation of a charge, the employee might be transferred to another. The processes for deciding posting and transfer are very elaborate and vary for each designation, and will be outside the scope of OIOS. However, the issue of relevant orders relating to transfer and posting would happen through OIOS. The hierarchy of designation and the relationship with organisational structure in the field audit offices is depicted below.

Designation in the streams relating to audit of State Governments	**Roles**	**Equivalent designation in the streams relating to audit of Union Government**	**Referred hereinafter as**
Principal Accountant General [31]/ Accountant General	Is the head of a field audit office	Director General (DG)/ Principal Director (PD)	HODs
Senior Deputy Accountant General / Deputy Accountant General	Is the head of a branch office / wing of a field audit office	Director / Deputy Director (DD)	Group Officers (GOs)
Senior Audit Officer / Audit Officer	Is the head of a branch of a wing in a field audit office or a branch office	Senior Audit Officer (SAO)/ Audit Officer (AO)	Branch officers (BOs)
Assistant Audit Officer / Supervisor	Is the head of a section	Assistant Audit Officer (AAO)	Section heads (SHs)
Senior Auditor / Auditor	Represents a unit	Senior Auditor / Auditor	Units
Welfare assistant, Hindi officer, Hindi translator, Clerks, DEO, MTS	work in a Section	Senior Auditor/Auditor, Hindi officer, Hindi translator, Clerk, DEO, MTS	

[30] The creation in OIOS of posts, and mapping of user roles to posts, is covered in the Organization Business Module.

[31] In some cases, in the past, the HoD has also been in the rank of ADAI

Personal Assistants	report to head of an office/branch office/wing		PAs

The hierarchy of designation in C&AG HQ is detailed below. The reporting hierarchy must be configurable.

- C&AG is the head of the IA&AD.
- Deputy C&AG (DAI) and Additional Deputy C&AG (ADAI) are heads of functional wings of C&AG and report to C&AG.
- PDs and DGs report to DAIs and ADAIs.
- Group officer report to PDs and DGs.
- SAO/AO/AAO[32] are called 'desk officers' and they report to PDs and DGs.
- Senior Auditors report to SAO/AO/AAO.

The cadre controlling authorities for different categories of employees are the authorities who control the promotion, transfer and posting of any employee; these are NOT necessarily the head of the office in which the employee is posted.

- With regard to posting of employees whose designation is Group Officer or above, the cadre controlling authorities directly post them to their respective postings.
- With regard to other designations, the cadre controlling authorities post them to an office. The office administration wing posts them to the functional wings of the field audit office after seeking approval from competent authority. The wing administrator allots them to a specific post after seeking approval from competent authority.

While the actual process of transfer and posting would be outside the scope of OIOS, the issue of orders after finalisation of the allocation would be done through OIOS. It is pertinent to note that allocation of audit assignments is not part of this sub-module and this is handled under 'Audit programme' sub-module.

9.1 Transfer of employees

The process of issue of orders of transfer of an employee from A to B (either from one office to another, or from one wing/ branch/ section/ dealing hand to another) is similar to that of posting order. The orders are followed by two events, i) getting relieved from A and ii) joining B.

9.2 Additional charge

A post or a charge can be assigned to only one employee. However, an employee might be given multiple charges, which is often termed as 'Additional Charge'. The reason for additional charge may be because of vacancy in a particular charge/post or that another employee in the office is on temporary absence / leave (with or without a standing arrangement). When an employee who has one or more additional charges logs into OIOS, the system will prompt the employee to choose the charge whose functions is about to discharged by him. The process of standing delegation of specific

[32] In the C&AG Office, the designations are Senior Administrative Officer; Administrative Officer; and Assistant Administrative Officer. Likewise, in the A&E Offices, the designations are Senior Accounts Officer; Accounts Officer; and Assistant Accounts Officer.

subset of activities using user roles and privileges using office-specific roles (Changes captured through audit trail).

Indicative business data relating to posting / transfer

- Posting to an office
  - Date of posting
  - Designation
  - Name of the office
  - Post to which the posting was done (for employees whose designation is equal to or above Group officers)
  - Nature of post (Original / Additional charge)
  - Date of relief
- Posting to a wing (for employees whose designation is below group officers)
  - Date of posting
  - Designation
  - Date of relief
- Posting within a wing to a branch/ section/ dealing hand (for employees whose designation is below group officers)
  - Date of posting
  - Designation
  - Nature of post (Original / Additional charge)
  - Date of relief

9.3 Actors involved

Many actors are responsible for maintenance of employee master and employee profile, including the employee.

Application administrator/Designated role (for designations equal to and above Group officers): After seeking approval from the competent authority, the application administrator issues orders of posting. AS mentioned earlier, this order gives the exact post of officers.

Cadre controlling authorities (for designations below Group officers): After seeking approval from the competent authority, the cadre controlling authority issues orders of posting an employee to an office.

Office administrator (for designations below Group officers): After seeking approval from the competent authority, the office administrator posts the employee to a wing.

Wing administrator (for designations below Group officers): After seeking approval from the competent authority, the wing administrator issues orders which allocate exact posts to the employee.

To clarify, the role of application/ office/ wing administrators is limited to implementation of postings in OIOS.

9.4 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below. However, the deliberations of transfer and posting committees, Departmental promotion committees etc. along with the actual process of seeking approval of competent authority for recruitment, promotion, posting and transfer will not be part of OIOS.

9.4.1 Issue of orders of recruitment

- Issue of orders of posting to an office.
- Issue of orders of posting to a wing.
- Issue of orders of posting to a charge.
- Issue of orders of transfer.
- Issue of orders of relief from charge/additional charge.
- Submission of joining report
- Issue of orders of additional charge/ standing arrangement.

Process	**Issue of orders of Transfer/Posting to an office, wing and to a charge**	
Process trigger	Decision of the posting committee or cadre controlling authorities or competent authority	
Process Inputs	Documentation of Decision	
Process Outputs	Posting order to an office/wing/charge	
Actors involved in the Business Process	**Actor**	**Function**
	Approval by competent authority	1. Posting to an office. 2. Relieving from office (in case of transfer)
	Office administrator	3. Posting to a wing 4. Relieving from wing (in case of transfer)
	Wing administrator	5. Posting to a specific charge 6. Relieving from specific charge/additional charge (in case of transfer)
	Employee	7. Submission of joining report
	OIOS System	4. **Master Data Management**: Acts as single source of truth for all IA&AD Applications. 5. Generate alert for all concerned, whenever change is made 6. Maintain change history
	Service Delivery Channel: OIOS	
System Interfaces with Other Modules/ Sub Modules/ External Stakeholders	Open API based access for all IA&AD Applications	

10 Gradation list (02_04)

The preparation of the annual gradation list of office employees by cadre (by the concerned cadre controlling authority) and in order of seniority will be included. The indicative business data for maintaining information regarding promotion and gradation is listed as part of employee master.

The promotion process is very complex and cannot be integrated into OIOS. Hence, after the completion of the process, the orders can be issued through OIOS and related data could be maintained in OIOS.

10.1 Actors involved

The following actors are involved in maintenance of information relating to promotion and gradation.

- **Promotion data administrator** issues promotion orders through OIOS.
- **Gradation data administrator** maintains data relating to gradation and draws gradation list...
- **Employee** receives promotion orders and views gradation list.

To clarify, the function of these administrators is only to implement promotions in OIOS.

10.2 Activities envisaged in OIOS

The change management from AS-IS process to To-BE process involves the following.

- Addition of promotion details.
- Maintain meta-data relating to gradation.
- View gradation list relating to an employee or a field audit office.

11 Nominations for training / capacity building (02_05)

With an objective of capacity building, an employee of IA&AD is trained at various levels. The training is provided by one or more of the following entities.

- National level training institutions of IA&AD such as National Academy of Audit and Accounts, iCISA, iCED, etc.,
- Regional training centres of IA&AD such as RTIs and RTCs.
- Trainings held by individual field audit offices.
- Specialised in-house trainings in functional wings of field audit offices.
- Training through external institutions (within India/ Abroad) such as IIMs, GAO, etc.,

Hence, the training received by an employee can be classified as the following.

- 'Institutional training' which will include trainings and workshops imparted by external agencies (within India or abroad), national level institutions, regional training institutes and centres. Under the institutional training, the annual training calendar is generally formally prepared along with master list of courses offered in a year. In some cases, especially training through external agencies, the training may be planned at short notice and not form part of the annual training calendar.
- 'Local training' which will include training and workshops given by the C&AG HQ, individual field audit offices and in-house trainings. Though some part of local training may be calendar based, most of the training is need based and hence ad hoc.

The information regarding nominations, exemptions for training, trainings attended for an employee would be captured in this sub-module. OIOS would provide the facility for the institutions that offer training within IA&AD to maintain the training calendar and modify them as and when necessary. It is important to note that the process of creation of training calendar including RAC meetings will not be captured in OIOS at present. However, documents may be uploaded by the training institutions, wherever necessary. IA&AD is also planning to invest in an e-learning platform. OIOS should facilitate API based integration with the e-learning platform and also provide scope for maintaining class-room training (especially if the same is not included in e-learning platform).

Indicative business data for nominations for training / workshop

- Nature of training (Institutional – within IA&AD/ External, Local, In-house)
- Institution name (If the nature of training is institutional, the list of names gets restricted to pre-defined institution from master data)
- Name of the training (If the nature of training is institution, the list of training courses[33] gets restricted to training courses from the training calendar of the selected institution) and category of training (from a master list)
- Dates of training
- Date of nomination
- Date of acknowledgement of nomination
- Was exemption sought for?
- Date of application of exemption
- Was application accepted/rejected?
- Date of approval/rejection of exemption application
- Post-training feedback from trainee/ Supervisory officer to training institution

11.1 Actors involved

- **Nominating institution:** The institutions will maintain data relating to the annual training calendar. The institutions will either nominate officials or request for a specific number of nomination slots from the office.
- **Nominating office:** The nominating office is responsible for nominating the officials for the in-house courses or as a response to request from nominating institution.
- **Nominee:** The nominee acknowledges the nomination or alternatively requests for an exemption.
- **Exemption approving authority:** The competent authority who can approve or reject applications for exemption receives the application and communicates the decision to the Nominee.

11.2 Activities envisaged in OIOS

- Maintaining training calendar by the training institutions.
- Nomination of an employee for a training by training institutions or nominating offices.
    - Subsequent issue of notification to the employee
        - Acknowledgement of notification by the employee or
        - Application for exemption
- Receipt of exemption application by competent authority
    - Approval of exemption request
        - Subsequent issue of notification to the employee and his acknowledgement of receipt.
    - Rejection of exemption request

[33] Some of training courses conducted might also include external participants. This information would be maintained by OIOS.

        - Subsequent issue of notification to the employee and his acknowledgement of receipt.
- Post training feedback (on training outcomes) to training institution

12 T&M phase of personnel module

The following sub-modules are part of the T&M phase.

12.1 Other administrative nominations (02_06)

Other than training, the employee is also nominated for various other administrative activities both for local activities and activities across field audit offices. OIOS would maintain a nomination type along with nomination category master, which would be maintained by the application administrator. An illustrative list of nomination types (a phased approach to implementation would be followed) have been listed below; many of these nomination types represent restricted or classified information, and a decision may be taken later to capture or NOT to capture them in OIOS.

The process leading up to the decision for nomination will NOT be captured in OIOS.

Nomination types[34]
Foreign assignments
Transfer and posting committee
Cash verification
Departmental promotion committee
Purchase committee
Sports-quota recruitment
Physical verification of IT assets
Committee for prevention of sexual harassment at workplace
Review of Group B officers under 56 (j)
Invigilation officer of examination
Presiding officer for examination
Setting of question paper
Examination of answer sheets
Inspection wing party
Others

The indicative business data relating to administrative nominations are the following.

Indicative business data relating to administrative nominations

- Nomination type
- Nominated by
- Dates of nomination
- Date of communication of nomination
- Date of acknowledgement of nomination

For the nomination types, where exemption information is required to be captured,

- Was exemption sought for?

[34] Many of these nominations are confidential, and a decision may be taken later to exclude such nominations. Also, the process leading to nominations will not be covered in OIOS.

- Date of application of exemption
- Was application accepted/rejected?
- Date of approval/rejection of exemption application

12.1.1 Actors involved

- **Nominating office:** The nominating office is responsible for nominating the officials for the various administrative activities.
- **Nominee:** The nominee acknowledges the nomination or alternatively requests for an exemption.

12.2 Leave (02_07)

The workflow involved in applying for and processing of leave (including computation and carry forward of the balance of leave standing to the employee’s credit) may be taken up during the T&M phase. Leave may be of different types – Earned Leave; Half Pay Leave; Commuted Leave (on Medical Grounds); Extraordinary Leave with/ without Medical Certificate; Child Care Leave etc.

12.3 Tour (02_08)

The programme relating to audit execution would be captured in 06_01: Audit Programme module. However, other non-audit related tour programmes and processing of tour claims may be taken up during the T&M phase.

12.4 Personnel Claims (02_09)

The workflow involved in application, process and approval of various personal claims (Travelling Allowance, Children Education Allowance, Medical reimbursement, Leave Travel Concession, sanction of various short term and long-term advances to office employees) may be taken during the T&M phase. It may also be explored to integrate or use applications of NIC, with the above functionalities.

03 Auditee Universe

This module will aid in maintaining a master of list of auditable entities under the mandate of C&AG ("who to audit"). It will also assist in managing the allocation of auditable entities to the field audit offices in the organisational structure (office/ wing/ branch/ dealing hand). This, along with organisation structure, defines the record-based permissions and workflow configurations[35]. The module also provides a platform to store configurable fields for each field audit office for each auditable entity. The module is divided into three sub-modules, viz., Universe master, Universe allocation, Universe profile.

13 Auditee Universe Master (03_01)

The Auditee Universe of IA&AD is the set of all entities of the Union Government and State/UT Governments that come under the audit jurisdiction of Comptroller & Auditor General of India, as defined by the authority in C&AG, DPC Act, 1971. Thus, the Auditee Universe consists of the following categories of auditable entities listed below. The Auditee Universe is hierarchically organized.

Union Government	State/UT Government	International[36]	Others
• Apex / constitutional bodies • Ministries • Departments • Attached and subordinate offices • Departmental Undertakings	• Apex / constitutional Bodies • Departments • Attached and subordinate offices • Departmental Undertakings • •	• Embassies and other equivalent offices • Other international offices of Union/ State Governments and Government-controlled entities	• Autonomous bodies and authorities of various kinds • Government companies (including Deemed Government Companies) • Statutory Corporations • Autonomous District Councils[37] • Panchayati Raj Institutions (PRIs) • Urban Local Bodies (ULBs) • Other entities whose audit is "entrusted" to the C&AG or otherwise covered by C&AG's mandate

[35] In some cases, workflow configuration could also be based on Ministry/ Department, in addition to the other parameters specified.

[36] Assignments involving audit of international organizations etc. are currently not proposed to be covered under OIOS.

[37] Falling under C&AG's audit jurisdiction in terms of the Sixth Schedule to the Constitution

Another method of categorization of auditable entities followed in the Department is by the relevant section of the C&AG's DPC Act, 1971[38] under which the audit mandate is derived; this needs to be mapped into OIOS:

- Audit under Section 13 – Audit of Union and State Governments (Expenditure)
- Audit under Section 14 (Section 14(1) and Section 14(2)– Audit of bodies and authorities substantially financed by Government
- Audit under Section 15 – Access to books of bodies and authorities receiving grants and loans from Government
- Audit under Section 16 – Audit of receipts of the Union and State Governments
- Audit under Section 17 – Audit of accounts of stores and stock maintained by any office of the Union and State Governments
- Audit under Section 19 (1) – Audit of Government Companies (including Deemed Government Companies)
- Audit under Section 19 (2) – Audit of Corporations established by or under law made by Parliament
- Audit under Section 19(3) – Audit of Corporations established by or under law made by State/ UT Legislature
- Audit under Section 20 – Audit of bodies or authorities entrusted to C&AG
- Others[39]

Each of the field audit offices in the IA&AD have a specific auditee jurisdiction, covering a subset of the entities which becomes the 'Auditee Universe' of the field audit office. Some of the auditable entities come under the audit mandate based on certain specific conditions such as, audit under Section 14 of C&AG's DPC Act. In such cases, the auditable entity might come under C&AG's audit mandate in one year and might fall out of audit mandate after a few years and then come back again. Correspondence in this connection, as well as correspondence for audit under Section 20 is to be captured as attachments/ supporting documentation.

One field audit office can audit many auditable entities. One auditable entity (and/or its sub-entities) may, in some cases, be audited by many field audit offices. Since the field audit offices would be entering their auditee universes individually, this may result in 'duplicates' in the auditable entities. Such duplicates may need to be resolved[40], by using the link to the Government Directory etc.

The field audit offices of IA&AD follow various methods to collect information about newly created entities or their closure.

a) Periodical communication with auditee entities or higher-level entities (typically with the Ministry/ Department/ Directorate/ Commissionerate[41])
b) Reconciliation with GoI web directory

[38] The C&AG's DPC Act is available at https://cag.gov.in/content/dpc-act-cags-duties-powers-and-conditions-service

[39] Including audit of the accounts of private entities, not normally within the audit mandate of CAG, if the entity has been allowed the commercial use of scarce natural resources under the terms of license, which requires the entity to share a part of the revenue so generated with the Government.

[40] Resolved does not necessarily mean removed; flagging could address this.

[41] Such information may also be collected during audit of the Ministry/ Department/ Directorate/ Commissionerate.

c) Reconciliation with DDO[42] Master maintained by different states in their local Integrated Financial Management System (IFMS)[43] and/or DDO Master maintained in the VLC System[44] of the A&E Office
d) Internal Crowd sourcing (Ad-hoc method, meaning as and when it comes to notice)

These processes are outside the OIOS ecosystem. However, it is envisaged to provide for viewing information sourced from GoI web directory and DDO Masters (VLC, Treasury and IFMS systems of the state within OIOS.

After processing the information from the above methods, the wing administrator / office administrator adds new entities / archives or closes entities when necessary, after seeking approval from competent authority. The attributes are also modified if required. OIOS would provide for ability to view history of changes made to attributes of the auditee entity, by users with privileges.

When the auditable entity undergoes a re-organisation (splitting or merging), OIOS should provide for a functionality to maintain link between old and new auditable entities. The following activities would be undertaken by the administrator concerned. **It is important to note that OIOS would not do this automatically**.

Merging of auditable entities: The administrator would create the new 'merged' auditable entity. The administrator then relinks the sub-entities of the old auditable entities to the new 'merged' auditable entity. The old auditable entities are then closed citing reason of re-organisation.

Splitting of auditable entities: The administrator would create the new 'split' auditable entities. The administrator then links/apportions the sub-entities of the old auditable entities to the new 'split' auditable entities. The old auditable entity is then closed, citing reason of re-organisation.

The attributes of any entity in the Auditee Universe have been listed in the indicative business data.

[42] DDO – Drawing and Disbursing Officer – an officer of the Union/ State Government who is authorized to draw bills and make payments on behalf of Government. All DDOs will be auditable entities of the C&AG, but several auditable entities (e.g. Government Companies, autonomous bodies etc.) may not be DDOs.

[43] Or the PFMS in respect of DDOs of the Union Government

[44] Voucher Level Computerization System of the A&E Office under the C&AG is used for compiling and finalizing the monthly and annual accounts of the State Governments, as well as subsidiary accounting information.

Indicative business data of auditee universe[45]

- Field audit office who is maintaining the auditable entity
- A code that uniquely identifies an auditable entity
- The name of the entity
- A short description
- Category and sub-categories (Configurable master data)
- Contact address including street address, village, taluk, district, state, pin code[46]
- Geographical location (Latitude and Longitude)
- Contact information including phone, email-id and website
- Section(s) of DPC Act under which the entity is audited
- Supporting documentation regarding inclusion in Auditee Universe
- Reporting to (i.e. unique ID of auditable entity to which this entity reports. This enables maintaining hierarchy of the auditee universe)
- Date of creation of entity
- Date of closure of entity
- Date of addition of entity to the Auditee Universe
- Date of removal/de-activation of entity from the auditee universe
- Remarks for removal/de-activation of entity from the auditee universe.
- Default classification (Apex auditable entity, audit unit, implementing unit)[47]
- Link to old auditable entity (in case of reorganisation)
- Mapping of Budget Grants to the auditable entity
- Mapping of DDOs to the auditable entity
- Link to the entity in the Government directory (To handle duplicates in auditee universe master)
- Wing/ Branch/ Dealing hand in the field audit office (Triggers record based permission)
- History of jurisdiction (for auditable entities which keep failing in and out of the jurisdiction)[48]
  - When did the auditee come under the C&AG's audit mandate?
  - When is the auditee likely to fall out of the audit mandate? (Useful for reviewing audit mandate periodically)
  - When did the auditee actually fall out of the audit mandate?

13.1 Actors involved

The office administrator / wing administrator or any user with privilege to manage the auditee universe master data would be able to maintain auditee universe.

[45] Certain fields of the auditee universe need to be stored in multiple languages. For example, the name and address of the auditee entity may be stored in English as well local languages. The exact list of multi-language fields would be decided during the sprint planning. The input of the multiple language will be through transliteration facility. For example, when the user types Namaste, the input tool gives various Hindi words with the most probable one (नमस्ते) in the top.

[46]The village, taluka/ block, district and state masters would be collected from Local Government Directory (LGD) https://lgdirectory.gov.in/ as a service.

[47] The IA&AD has adopted a classification of auditable entities into Apex Auditable Entities (AAEs), Audit Units (AUs) and Implementing Units (IUs). However, this classification may, sometimes, vary with the specific audit assignment; hence, we are using a term "default classification".

[48] Correspondence with the Government (and responses thereto) with regard to such auditable entities will also be captured as attachments in OIOS.

13.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Add new auditee entity under the jurisdiction
- Remove auditee entity from jurisdiction
- Maintenance of details of auditee entity based on jurisdiction

Process	**Maintenance of auditee universe master**	
Process trigger	New information obtained from auditee, other officials of field audit office, arising out reconciliation with GoI web directory and DDO directory	
Process Inputs	Information regarding a new entity or modification of attributes of an entity or closure of an entity	
Process Outputs	Up-to-date auditee universe master	
Actors involved in the Business Process	**Actor**	**Function**
	Office administrator or Wing administrator or User with privileges	8. Make the necessary changes. 9. Upload and/or link attachments such as documentation of change.
	OIOS System	7. **Master Data Management**: Acts as single source of truth for all IA&AD Applications. 8. Generate alert for all concerned, whenever change is made 9. Maintain change history
	Service Delivery Channel: OIOS	
System Interfaces with Other Modules/ Sub Modules/ External Stakeholders	Open API based access for all IA&AD Applications	

14 Auditee Universe profile (03_02)

Each of the field audit office in the IA&AD have each been allotted a subset of the entities which becomes the 'Auditee Universe' of the field audit office. The auditee master data captures the common minimum data elements that is to be maintained uniformly across IA&AD. However, as part of auditee universe profile, the field audit offices would be able to maintain their own set of configurable fields. The fields may have temporal in natures. That is, the values change over time. For example, a field audit office might want to prepare an auditee universe profile in the following manner.

- Budget Grant (Primary)
- Additional grants operated by the auditable entity

Alternatively, the field audit office may like to maintain a specific set of fields for specific set of auditable entities which are similar. For example, a field audit office may wish to store numbers of primary schools and secondary schools that come under the jurisdiction of all District Educational Officers under its audit jurisdiction.

In order to facilitate such special needs, this sub-module would include a feature for defining profile templates (a set of fields that would be used by the field audit offices) and using the same to store custom profile information regarding their auditee universe. In theory, the sub-module must be flexible enough to enable field audit office to add fields for an auditable entity or a set of auditable entities on the fly. Any original / additional configuration would be reviewed by the application administrator before being submitted to the approval process by competent authority.

It is pertinent to note that any other semi-structured/unstructured information such as documents would be stored in the Auditee information system as part of Knowledge Management System of OIOS, and NOT as part of this Business Module.

Indicative business data for auditee universe profile
What are the templates for profile? What are the data elements in a template?
What templates are applicable to an auditable entity?
What are values of data elements of an auditable entity?

14.1 Actors involved

The office administrator / wing administrator is responsible for creating the templates, modifying the templates, attaching template to an auditable entity and entering the data for the auditable entity. However, the collection and entering of data may also be crowd sourced by the field audit teams.

14.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Create a new template with data elements.
- Attach one or more templates to auditable entities.
- Capture data for the auditable entity in the attached templates.
- Detach one or more templates with auditable entities.
- Modifying the created template.

04 Audit Planning

This business module aims at providing a platform for preparation of annual audit plans (with rolling plans) for each field audit office and IA&AD, along with the documentation of the planning and topic selection process at various levels. The module can, in future, provide a platform for preparation of strategic audit plans of each field audit office and IA&AD and also scope for performing the risk assessment for planning within the module.

15 Annual Audit planning (04_02)

The audit mandate of the C&AG is vast, and the number of auditee entities that could be covered in audit and the number of topics/ themes that could be covered through performance/ theme-based compliance audits in a financial year is much, much larger than the available human resources within C&AG for audit. Hence, **audit planning** is necessary to prioritize "what to audit" in a given timeframe, after doing a risk assessment, considering the available human resources, and also taking note of mandatory (financial attest audit) assignments that have to be performed.

Audit planning takes place at two levels:

- Strategic Audit Planning (currently not prepared) – long-term planning for the IA&AD as a whole as well as individual field audit offices, typically covering a five-year time frame;
- Annual Audit Plan and Rolling Plans – short term annual audit plan for IA&AD and Field Audit Offices, accompanied by tentative, less detailed, rolling plans for the next two years.

The detailed planning and drawing up of audit guidelines for individual audit assignments ("how to audit") and the audit programme (short-term, detailed day-by-day audit programme including assignment of specific personnel) are covered in other business modules.

15.1 Annual Audit Plan and Rolling plan

The purpose of the Annual Audit Planning exercise is to identify and prioritize audit assignments to be carried out in the upcoming year and allocate resources for the same. While preparing the annual audit plan for the upcoming year, tentative annual audit plans for the subsequent two years (termed as 'rolling plans') are also prepared. The annual audit plan and rolling plan would be prepared at the field audit office level, and then consolidated at the IA&AD level.

The annual audit plan and rolling plan for each field audit office is prepared by them in the third quarter of the previous financial year, with approval from C&AG's office expected before the commencement of the next financial year. For example, the annual audit plan of 2020-21 of a field audit office and its rolling plans of 2021-22 and 2022-23 are prepared in the third quarter of 2019-20 and would be approved by 31.03.2020. In case of a large field audit office having more than one functional wing, the annual audit plan and rolling plan for the wings may be prepared wing-wise separately and then consolidated for review.

The annual audit plan is constrained by the expected available manpower for field audit during the financial year (i.e. excluding audit resources used for non-audit related activities and at the field Headquarters, considering the number of working days in the financial year, and after making necessary deductions for training, leave, etc.).

The assignments / activities that are carried out by a field audit office during a year and are therefore considered for inclusion in the Annual Audit Plan/ Rolling Plans includes one or more of the following.

Performance Audits

i. All-India / Centralized Performance audits[49].
ii. Performance Audits co-ordinated across different States[50] with a nodal Audit Office;
iii. Performance audits on topics selected locally by the Field Audit Office through a risk assessment process and/or pilot audits.

Financial Audits

i. Financial attest audits of the accounts of the Union and State Governments and UTs with Legislature;
ii. Financial attest audits[51] of accounts of corporations, Government-owned companies, bodies and authorities expected to be received during the year. It is normally not possible to accurately estimate the receipt of accounts for financial audits. The process has been detailed further in the next section.

Compliance Audits

i. Compliance audits on specified subject matters or themes, where themes are selected through a risk assessment process and/or pilot audits.
ii. Other "non-subject matter specific" compliance audits.

Others

i. Pilot audits on specific topics / themes to ascertain feasibility for future performance audits/ theme-based compliance audits.
ii. Independent assignments for collection of data on auditee entities.
iii. Collection of additional documentation to support/ strengthen/ validate findings or earlier audits[52]

Thus, the output of the Annual Audit Plan will be a list of audit assignments in the Annual Audit Plan; the audit assignments may specify the complete set of auditable entities in each assignment, or may not. This also does not mean that new audit assignments (not figuring in the Annual Audit Plan) cannot be programmed; just that when this happens, this must be flagged explicitly as a deviation from the Annual Audit Plan. The workflow for (either ex ante or post facto) review/ approval of such deviations will be configured separately.

[49] All-India Performance Audits typically cover centrally sponsored schemes or projects where both the Central Government (usually for overall planning, fund allocation, and monitoring) and State Governments (usually for detailed planning, matching fund allocations, implementation and State/ local-level monitoring) are involved, with the Central Audit Office acting as the nodal office, but generally two sets of Audit Reports (to the Parliament and State Legislatures) are envisaged. Centralized Performance Audits are typically undertaken in the Central Revenue Audit, Railway Audit etc. streams where one office acts as a nodal Audit Office.

[50] The difference vis-à-vis All India Performance Audits is that no Central Audit Report is envisaged. This approach has been recently introduced.

[51] depending on the field audit office and its audit jurisdiction, responsibility as principal auditor or sub-auditor

[52] Usually undertaken in respect of audit findings tentatively identified for further processing for possible inclusion in the C&AG's Audit Report.

In some cases, e.g. Defence audit, the Annual Audit Plan may also list the individual procurements/ contracts (contract award and/or contract management) or groups of procurements/ contracts as audit assignments to be covered, based on a master list of procurements (capital and revenue procurements) collected by the Field Audit Office from the auditable entity at an appropriate level. The audit units to be visited may be "mapped" back to the contracts to be scrutinized.

15.1.1 Sub-assignment under each audit assignment

There are various milestones or activities (sub-assignments) that a field audit office undertakes for each type of audit assignment. For example, the activities for specific assignment types are illustrated in the Table below. The list of assignment types would be drawn up as master data. These sub-assignments may be added during planning, design or execution phase of audit. The list of activities for each assignment type would also be maintained as part of master data by the application administrator.

Assignment type	Sub-assignments
Audit of accounts of Government / Deemed Government Companies as a supplementary auditor	• Additional Sub-directions (in addition to directions issued by C&AG Office) • Meeting with Statutory Auditors / Company Officials • Receipt of Accounts • Verification at HQ of field audit office •
Performance audit	• Pilot study (Link to an audit assignment) and other work to finalize audit guidelines for a future audit assignment •
Three-phase audit of accounts of Government companies as supplementary auditor	• First Phase - Review of accounting policies (before finalization of accounts) • Second Phase - Audit comments/ observations on draft accounts (before accounts are adopted) • Supplementary audit comments on finalised accounts

The indicative business data relating to the annual audit plan of field audit offices is listed below.

Indicative business data relating to Annual audit plan of field audit office

- Name of the office
- Financial year
- What are the topics/ themes/ subject matters for the audit assignments to be taken up for this year?
- Documentation of process involved in the selection of the assignments through a qualitative and/ or quantitative assessment of audit risk.

Indicative business data relating to each audit assignment in the annual audit plan

- Name of the assignment
- Type of the assignment (Compliance audit, performance audit, IS audit etc.)
- Documentation of process involved in selection of focus areas through a qualitative and/ or quantitative assessment of audit risk. The documentation also includes the outcome of the selection process which is the list of focus areas and broad audit objectives.
- In which audit report will the observations of the assignment be featured in?

- Envisaged activities and timelines
- List of possible auditable entities to be audited under the assignment
- Default classification of key documents attached

Indicative business data relating to each sub-assignment of an audit assignment in the annual audit plan

- Type of sub-assignment
- Planned start date
- Planned end date
- Actual start date
- Actual end date
- Attachments relating to sub-assignment

15.1.2 At IA&AD level

The annual audit plan and rolling plan for the IA&AD as a whole represents a consolidation of the topics/ subject matters/ themes selected for performance audits and theme/ subject matter specific compliance audits, covering.

i. All-India/ Centralized Performance audits on selected topics and other co-ordinated Performance Audits.
ii. Local Performance Audits and Subject-Matter/ theme-based compliance audits.

Indicative business data relating to Annual audit plan of IA&AD

- What are the topics/ themes/ subject matters for the assignments to be taken up for this year?
- Documentation of process involved in the selection of the assignments through a qualitative or quantitative assessment of audit risk.

Indicative business data relating to each assignment in the annual audit plan

- Name of the assignment
- Which field audit offices are participating? Which is the nodal office?
- Documentation of process involved in selection of focus areas through a qualitative or quantitative assessment of audit risk.
- Envisaged milestones and timelines

15.1.3 Planning of financial audits

Financial audit is the process of expressing an audit opinion (as the primary auditor) on the financial statements of the auditable entity (Union/ State Government, corporation, body or authority), or where the C&AG is a secondary auditor (for Government-owned companies, where a Chartered Accountant is appointed as the primary auditor), giving supplementary comments on the financial statements of the auditable entity.

Where the C&AG is the primary auditor of an auditable entity, financial attest audit of the accounts of the auditable entity is mandatory. However, for financial attest audit of Government owned companies, upon receipt of accounts for an auditable entity, a field audit office will assess, in accordance with criteria specified by the Headquarters Office, the risk associated with the accounts submitted by the auditable entity. If the audit risk is not significant, then the field audit office would consider issuing a non-review certificate with approval from the competent authority. However, if the audit risk is significant, the accounts are subjected to financial audit.

It is important to note that the planning and scheduling activity of the field audit office is heavily dependent on whether and when the accounts are received; the timing of such receipt is variable. The OIOS system would track the receipt of accounts, and consequently, the non-receipt or arrears of accounts. Thus, the field audit offices are generally not in a position to ascertain exactly the number of financial audits that are to be undertaken beforehand during a year. However, the field audit offices would be able to ascertain the number of accounts awaited at any given point of time.

15.2 Actors involved

The competent authority to approve the annual audit plans of IA&AD and field audit offices is the Comptroller & Auditor General of India with regard to the subject matters/ themes taken up for audit (to be potentially considered for inclusion in the C&AG's Audit Report), and the respective functional wings of the Headquarters Office with regard to the other elements of the annual audit plans of the field audit offices. The planning process of the field audit office would generally involve an 'Audit planning group' consisting of relevant stakeholders. The composition of the 'Audit planning group' will vary from field audit office to field audit office. The opinions of the members of the group and the deliberations made during the meetings of the group form a strong basis for preparation of the annual audit plan. Apart from the 'Audit planning group', the following are the actors involved in the preparation and approval of annual audit plan.

The C&AG has an Audit Advisory Board, including external experts, to provide independent advice, among other things, on the topics/ themes to be taken up for audits. Likewise, the Field Audit Offices dealing with audit of State Governments have State-specific Audit Advisory Boards.

Preparers: The annual audit plan preparers would have the responsibility to collate inputs received from various sources and prepare a draft annual audit plan. Depending on the size of the office, there might be more than one preparer. For example, one per functional wing of FAO or one per audit report published by a FAO.

Reviewers: The annual audit plan is then examined by several reviewers who become part of 'proper channel' or 'workflow'. The reviewers provide feedback / comments / queries that are to be either attended by reviewers at a lower level or the preparer.

Approver: The final approval of annual audit plan is given by competent authority.

The flow of the work between preparer, reviewer and approver is very iterative and goes on for several rounds until the finalisation and approval of annual audit plan is complete. Only the final, formal approval of the Annual Audit Plan is intended to be captured in OIOS.

15.3 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Document review / approval process of working papers during initial preparation/mid-term reviews of annual audit plan document for field audit offices and IA&AD as a whole.
- Maintenance of data elements which are essential for MIS reporting after approval / review of strategic plans.

Process	**Preparation / Mid-term review of annual audit plan of IA&AD or field audit office**

<table>
<tr><td><b>Process trigger</b></td><td colspan="3">Time based trigger as the process is repeated periodically on an annual basis (Outside OIOS)</td></tr>
<tr><td><b>Process Inputs</b></td><td colspan="3">Strategic audit Plan of the previous year (optional), Plan Documents, Departmental Outcome Budget, Annual Reports of Government Department, Information from Auditee IS such as schemes, activities, budget, details of expenditure, parameter-based risk assessment, Past Audit Reports and Follow Up, Media clippings and External Reports</td></tr>
<tr><td><b>Process Outputs</b></td><td colspan="3">Minutes of the meeting, working papers and strategic plan</td></tr>
<tr><td rowspan="6"><b>Actors involved in the Business Process</b></td><td><b>Actor</b></td><td><b>Function</b></td><td><b>Service delivery channel</b></td></tr>
<tr><td>Audit Advisory Board and Audit planning group</td><td>Meetings and discussions</td><td>Traditional (Outside OIOS)</td></tr>
<tr><td>Planner</td><td>Development / Review of annual audit plan</td><td><b>OIOS</b></td></tr>
<tr><td>Reviewers in proper channel</td><td>Reviews annual audit plan and provides feedback/comments</td><td><b>OIOS (Document workflow)</b></td></tr>
<tr><td>Approver</td><td>Provides feedback/comments and approves annual audit plan</td><td><b>OIOS (Document workflow)</b></td></tr>
<tr><td>OIOS</td><td>Saves various versions of the annual audit plan along with necessary data elements</td><td><b>OIO</b>S</td></tr>
<tr><td><b>System Interfaces with Other Modules/ Sub Modules/ External Stakeholders</b></td><td colspan="3">Open API based access for all IA&AD Applications</td></tr>
</table>

16 Parametric risk analysis (04_03)

The determine the audit risk i.e. the probability of material irregularity assists IA&AD in prioritising focus areas of audits, auditable entities and transactions to be test checked. One such methodology to measure audit risk is based on a parametric approach. Let us consider the case of risk analysis of auditable entities. In order to evaluate the risk associated with each auditable entity, certain parameters ('risk parameters') are defined. The parameters may be financial or non-financial, quantitative or qualitative.

The C&AG's Auditing Standards stipulate that auditors shall manage audit risk (the risk that the audit report may be inappropriate). Conventionally, any audit risk model has three components – (a) inherent risk – the inherent risk of misstatement/ non-compliance/ error etc. in the class of units/

transactions being covered in audit (b) control risk – the risk that control mechanisms within the auditee entity fails to prevent, detect or correct such instances of misstatement/ non-compliance/ error and (c) detection risk – the risk that audit procedures fails to detect instances of misstatement/ non-compliance or error.

With regard to audit planning – i.e. selection of audit assignments and auditee entities for audit[53], the draft risk assessment model developed by C&AG Headquarters categorized risk parameters into two – inherent risk factors and control risk factors. There is a list of inherent risk factors and control risk factors prepared by C&AG Headquarters, which can be varied as appropriate by Field Audit Offices to suit their requirements. Likewise, the weightages assigned to inherent risk factors and control risk factors, which is used to generate a total weighted risk score for prioritization and selection of audit assignments and auditee entities, can be varied as appropriate by Field Audit Offices to suit their requirements.

The same sub-module can also be used for measuring risk of transactions using a parametric approach during audit execution.

16.1 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Creation of risk assessment activity.
- Create and add a risk parameter to the activity or re-use an existing risk parameter.
- Categorise the risk parameter as Inherent or Control.
- Assign weightages to the risk parameters.
- Configure the formula for calculation of total risk.
- Upload a list (csv, Excel) the auditable entities or transactions for which risk is to be measured or alternatively choose a sub-set of auditable entities from the auditee universe.
- Upload risk parameter values (csv, Excel) for the auditable entities / transactions.
- Trigger calculation of total risk score.
- View/Analyse the risk scores.
- (Optional) Feed the result as an input to statistical sampling to select auditable entities / transactions.
- Link the risk assessment activity to an audit assignment.

17 T&M phase of Audit planning module

The following sub-modules would be taken up in the Time & material phase of OIOS.

17.1 Strategic audit plan (04_01)

Strategic plan represents planning from a long-term perspective. This plan includes focus areas of audit that is envisaged in the next three to five-year perspective. The formulation of strategic audit plan is a bottom-up process and includes primarily identification of macro level key areas to audit. It also includes topics to be undertaken in each audit report by each field audit office mapped to the key

[53] The risks with regard to selection of transactions/ units within a performance audit or a theme-based compliance audit are considered to be part of "audit design" and are dealt with under that business module.

areas to audit[54]. Although, the strategic audit plan is currently not being prepared at the IA&AD level, it may be prepared by the individual field audit offices. Sometimes, the strategic audit plan may also be found as a 'basket/ portfolio of potential audit topics' in field audit offices. At present IA&AD does not have strategic audit plan though it was prepared in the past, and will be prepared in the future.

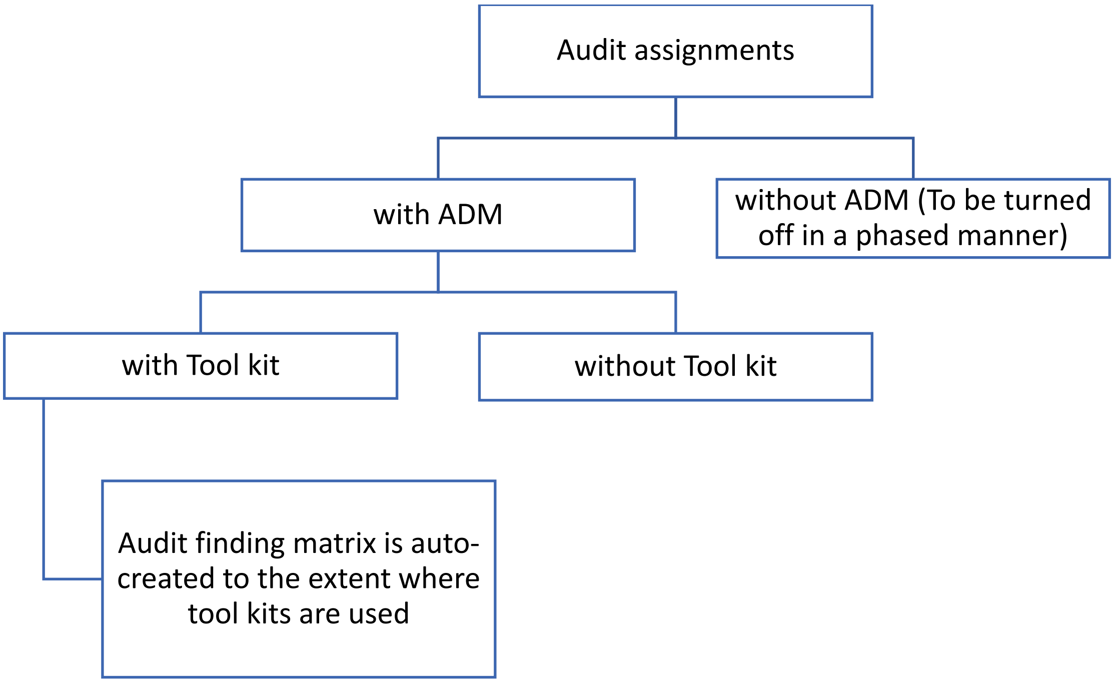
[54] A one-to-one mapping between the themes/ topics in the Strategic Plan and the Annual Audit Plan/ Rolling Plans is not envisaged. Rather, the mapping/ comparison will be qualitative.

05 Audit Design

18 Overview

This business module aims at providing a platform for preparing the micro level or detailed planning, i.e. designing an audit assignment. This design process for each audit process includes preparation of audit guidelines and selecting the auditee entities to be covered (including sampling approach for selection of units and transactions, where necessary). The process of preparation of audit guidelines involves the definition of audit scope (including the period of coverage), preparation of audit design matrix including design of audit objectives, audit sub-objectives (at multiple hierarchical levels, as necessary), and audit questions, as well as the criteria to be used, the sources of documentary evidence etc.

The design process may also include preparation of audit tool kits to collect necessary data that would assist in answering audit questions and consolidating such responses, and thus or attain the audit objectives / sub-objectives. It is important to note that the preparation of Audit design matrix for every audit assignment is not all pervasive as the change management of IA&AD to the approach in the 2016 compliance audit guidelines is still under way. Hence, the OIOS should allow[55] for non-ADM based audits.



Audit assignments
with ADM
without ADM (To be turned off in a phased manner)
with Tool kit
without Tool kit
Audit finding matrix is auto-created to the extent where tool kits are used

18.1 Process Description

The design of the audit assignment primarily involves two activities, viz., pilot audits in the field and desk review. The process of pilot audit is similar to an audit assignment, in terms of audit design and execution, and hence is not covered here. The process of desk review is described in the following

[55] This featured will be turned-off in a phased manner.

section. The desk review process uses inputs from the OIOS system, and the documentation of desk review process is captured in the form of audit guidelines.

18.2 Desk Review

Before the audit design, it is assumed that the theme/topic for the performance audit or theme-based compliance audit is clearly defined.

The preparation of audit guidelines includes:

- Defining the audit scope (i.e. what will and will NOT be covered in the audit assignment, including the areas of coverage and the period of audit coverage);
- Defining the audit objectives, audit sub-objectives (at multiple hierarchical levels, if necessary) and the audit questions;
    - ❖ For example, if one audit objective is “determine whether planning was adequate and effective”, determining whether the input data used for planning was reliable could be a sub-objective. Alternatively, there could be audit sub-objectives for planning at the State, District and Block levels, if planning is required to be done at all such levels.
- Creating the “Audit Design Matrix”, including not just the audit objectives/ sub-objectives and questions, but also the audit criteria and the sources of audit evidence.
- (Optionally) create one or more IT-based audit toolkits to collect data in answering the audit questions, and consolidating such responses to be able to answer the questions (and thus attain the audit sub-objectives and objectives)
    - ❖ Audit questions may be answered at one or more levels (e.g. for an audit of controls in production units and warehouses on manufacture and supply of alcohol, there may be questions to be answered at the level of the State Commissioner of Excise, and individual distilleries/ country liquor or IMFL bottling units/ breweries/ warehouses)
    - ❖ Questions may use “skip logic” for the next question, depending on the answer to the current question
    - ❖ Answers to audit questions may be in different formats – Yes/ No/ Partly (or one out of many choices); select multiple choices; quantitative; or purely qualitative
    - ❖ Most questions will have one or more supplementary fields for “remarks” or qualitative explanations to support the main answer
    - ❖ Hyper-linking or referencing is very important and necessary. Referencing for the basis of the question (e.g. the relevant section of the Liquor Excise Act) and also referencing for the supporting documentation[56] for the response (audit finding) to the audit question. Supporting documentation/ attachments may be in multiple formats (Word/ Excel/ PDF; photographs; scanned documents; even videos); metadata tagging of supporting documentation for easy retrieval is essential.

For designing the audit guidelines during the desk review, the designer shall collect and review various types of information from the OIOS KMS. These can come from multiple categories:

[56] We envisage that the supporting documentation (in multiple formats), with suitable metadata, will be stored in a Document Management System. However, this is a design decision for the SI.

- Audit Guidance (issued by C&AG Office and/or by Field Audit Offices) - Regulations; Auditing Standards, Auditing Guidelines, Guidance Notes, Practice Guides, Manuals
- ADMs and audit checklists/ toolkits prepared for similar assignments in the past by audit teams (either within the same Field Audit Office or other offices);
- Past findings about the auditee which is available in the records like earlier issued Inspection Reports, Pending IRs/Para(s), and more generally, BI/ analytics data from the audit and audit process data populated into OIOS over time
- Unstructured information about the auditees (e.g. GOs/ GRs; Budget papers; Annual/ long term Plans; DPRs; Procurement Documentation; Evaluation Reports), scheme/ program specific information (including scheme guidelines, scheme implementing information etc.).
- Structured information about auditees (financial and/or operational transaction data, MIS data etc.)

Part of the information may already be available in the KMS; other information which has been specifically collected for this audit assignment (either through the desk review or pilot study) shall be fed into the Knowledge Management System/ Data repository with metadata created and tagged Linking of all KMS documents/ information used for creating the Audit Design Matrix for an audit assignment (i.e. to know in which audit assignments this information has been used) shall be done. The users would be able to access the above required information from various components of OIOS and other multiple sources.

Another important aspect of audit design is the sampling approach and selection of auditee entities/ transactions for detailed field audit. The actual design of the sampling approach and the basis (E.g. which type of statistical sampling to use – Simple Random Sampling With/Without Replacement; Cluster or Multi-Stage Sampling; Probability Proportionate to Size Sampling and combinations thereof; determination of sample size etc.) will be done by the Field Audit Office with the assistance of statistical experts. The overall process of audit design is described in detail below.

Process	Audit Design Process – Preparation of audit guidelines	
Process Inputs	Desk review and / or pilot audit	
Process Outputs	**Audit Guidelines**: • Selection of auditable entities covered under the audit assignment and classification, including sampling approach • Determination of Audit Scope • Audit Design Matrix (ADM) • Audit Toolkit	
Actors involved in the Business Process	**Actor**	**Function**
	Audit Designer	Access KMS to Analyse Topic/subject specific information and Auditee Data (details provided in further sections)
		Prepare and update sampling methodology
		Desk review and pilot audit
		Prepare Audit Guidelines:[57] • Defining sampling approach, and selection and of auditable entities/transactions

[57] Audit Guidelines may be reviewed and updated during the Audit Execution; such updating should be facilitated by OIOS.

		- Audit Scope and - ADM - Audit Toolkits
	Reviewer	Reviews and approves audit guidelines
	Approver	Approval
System Interfaces with Other Modules/ Sub Modules/ External Stakeholders	**OIOS:** KMS, Auditee Universe, IR Repository, Media news Repository	
	External: Budget & Sanction Data, VLC Data; Auditee Entity Information System, if any	

19 Audit design matrix (05_01)

The next step is preparation of audit design matrix. An audit design matrix is a methodology through which an audit approach can be systematically designed. It also helps in scoping the audit assignment in a systematic manner. When an audit assignment is driven by a sound audit design matrix, then it paves way for a process or assurance-based audit. The approved audit design matrixes are pushed to a central library, where it is available for the employees of IA&AD to search, download, refine/ update and thus reuse.

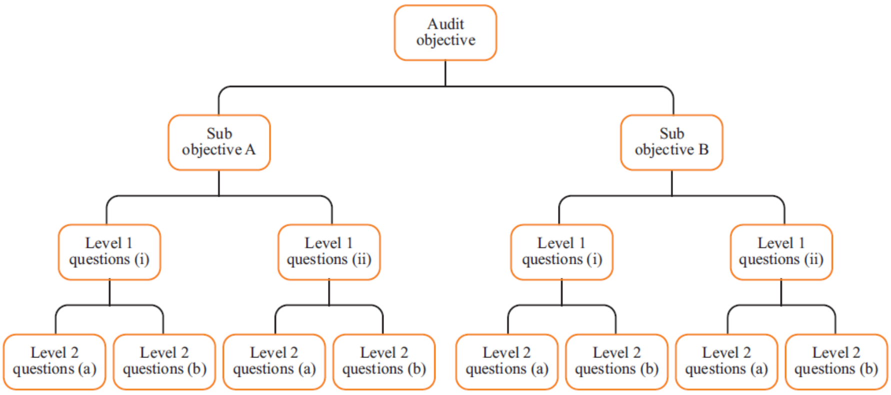


Figure 3: An illustration of audit design matrix

The indicative business data relating to the preparation of audit design matrix is listed below.

Indicative business data relating to preparation of audit design matrix

- What are the audit objectives?
- What are the sub-objectives under each audit objective? (optional)
- What are the audit questions under each sub-objective/objective?
- For each audit question or a sub-objective or an audit objective, the following design elements may be captured. If the design elements are designated at a higher level, say sub-objective, the design elements may be inherited by the lower level, i.e. audit questions.
    - What are the sources of audit criteria against which the current status is measured to answer the audit question (with hyperlinking facility to bookmarked sections of a document in KMS or the entire document)?

- What methodology has been chosen for data collection and analysis? For example, one of methodologies chosen for data collection and analysis is through audit toolkits[58] which is explained in the '**09: Data collection module**'. If methodology is audit toolkit, what are the various tool kits that are required for answering the audit question?
- What are the types and sources of audit evidence?
- What offices are to be visited in order to collect the audit evidence (restricted to the sub-set of auditee universe related to the assignment described in the section below)

19.1 Selection of relevant sub-set of auditee universe

The selection of 'relevant' sub-set auditee universe relating to the audit assignment includes selection of all auditable entities from which documents, records, data and information would need to be collected. The selection of auditable entities may be partially or completely through statistical sampling which is described in the next sub-module. It is important to understand that some of the auditable entities chosen might not be under the audit jurisdiction of the field audit office or its functional wings which is actually undertaking the audit. For example, consider a field audit office which has undertaken an audit assignment which is auditing a welfare scheme of Education Department of a state. The scheme aims at distribution of free laptops to class 12th students who are studying in Government schools. Though, the Department of Education is the implementing agency, the procurement of laptops for the purpose of this scheme might be a public sector undertaking under Information Technology Department which is under the jurisdiction of another field audit office.

Thus, there is a possibility that auditable entities of the assignment cuts across audit jurisdictions of field audit offices. OIOS should facilitate such selection along with notification process to the field audit office/functional wing, which holds the original jurisdiction. The selection process may be manual or by uploading a list of auditee entities (csv, txt, Excel) which were chosen as a result of risk assessment.

After the selection of the auditable entities relating to the audit assignment, the next step is to review their classification as 'Apex auditable entities', 'Audit units' and 'implementing units'. The default classification is captured as part of the auditee universe master data. However, the roles of the selected auditable entity might vary depending on the theme or subject matter considered under the audit assignment. Hence, OIOS would provide an opportunity to specify assignment-wise classification or allow the default classification, as the designer chooses to. Further, this selection and classification process is not a one-time event but can happen until the design stage is frozen.

Indicative business data relating to related subset of auditee universe

For each audit assignment,

- What are the auditable entities that are chosen for the assignment?

[58] Audit toolkits can also help in performing audit checks designed to achieve an audit objective or a sub-objective. They may also be used in answered one or more audit questions. It can also be a set of inter-related questions which need to be consistently asked and answered across selected audit samples or units. Audit toolkits are typically connected to the Audit design matrix. There is a many-to-many relationship between an element in ADM and Audit Toolkit. This means that one tool kit can answer one or more objective or sub-objective or question. Similarly, in order to answer one audit objective or audit sub-objective or audit question, many toolkits may be required.

- Date of inclusion of auditable entity in the audit assignment
- Date of removal of auditable entity from the audit assignment
- Is the default classification suitable for the assignment? If No, what is the classification with regard to the audit assignment?
- If the auditable entities do not fall under the jurisdiction of the functional wing of the Group officer/field audit office, a notification is issued to the office regarding the engagement.
    - Date of notification
    - Contents of notification
    - Date of receipt of acknowledgement from the other field audit office/its functional wing

19.2 Actors involved

OIOS proposes to capture only the final approved Audit Design Matrix and not the iterative process for development of the ADM.

- **Designer** proposes the audit design matrix (including selection of auditable entities under the audit assignment, classification) with the relevant design elements.
- **Reviewers** review the matrix and provides feedback.
- **Approver** approves the matrix.
- **Office administrator / wing administrator** of the field audit office under whom the audit jurisdiction of the selected auditable entities falls under.

19.3 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Selection of auditable entities for the audit assignment.
    - In case, where the jurisdiction does not fall under the designing field audit office / its functional wing, a notification is sent to the field audit office / its functional wing under whom the jurisdiction falls (not automatic but manual as the designer has to enter remarks explaining the scope of audit assignment for which the auditable entity is to be approached).
    - Acknowledgement of the other field audit office / its functional wing.
- Classification of auditable entities for the audit assignment.
    - Default classification or alternate classification as supplied by the designer.
- Preparation of audit design matrix.
- Review of audit design matrix.
- Approval of audit design matrix by the competent authority.
- Search for relevant audit design matrix stored in central library.
- Download relevant audit design matrix.
- Refine/ update the downloaded audit design matrix and reuse it for another assignment.

20 Sampling approach (05_02)

The designer may then apply statistical sampling to select the auditable entities and / or transactions that are to be subjected to audit. The actual sampling process happens outside OIOS in the initial releases. The functionality of being able to perform sampling within OIOS is to be taken up in Time & Material phase as described in the subsequent chapter. The indicative business data that are to be captured in relation to statistical sampling is listed below. This part of design apart from the regular reviewer would also be reviewed by an expert in statistics.

Indicative business data in relation to statistical sampling (to be captured as a Word Document)

For each assignment and each stage of sampling (in case of multi-stage sampling)

- What was the type/sub-type of sampling? (Simple random sampling -> with/without replacement, stratified random sampling, judgemental sampling (with justification), cluster-based sampling, Probability proportional to size (monetary unit, weighted contribution of different parameters, combination of multiple parameters)
- Description of the sampling
- What are the details regarding the sampling method?
- Details of how the actual sample is drawn, including starting seed number etc.
- Attachments (Documentation relating to sampling approach)

20.1 Actors involved

The following are the actors involved in statistical sampling (an iterative approach happens often). OIOS does not intend to capture the workflow for the statistical sampling, and will only capture the final approved/ agreed statistical sampling approach and the final statistical sample of auditee entities/ transactions as selected.

- **Designer** proposes a statistical sampling methodology relevant to the audit assignment along with the data and results.
- **Reviewer** reviews the data and results and provides feedback.
- **Statistics Expert** (Statistical Advisor or other Expert) reviews the data and results and provides technical opinion.
- **Approver** approves sampling methodology with assistance from the technical opinion.

20.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Proposal of the sampling methodology.
- Review of the sampling methodology by design reviewer.
- Review of the sampling methodology by the Statistical Advisor.
- Approval of the competent authority.

21 Audit guidelines (05_03)

The audit guidelines is a document which includes the documentation of the audit design of the document. It includes the following components.

a) A word document with annexures explaining scope of audit, period of coverage, sampling approach and methodology, sub-assignments (timelines and milestones), routine checklists (not filled through tool kits).

b) Link to Audit design matrix ((including selection of auditable entities under the audit assignment, classification).

c) Link to sampling approach approved (or to be approved) by competent authority.

This document is subjected to an approval workflow which includes functional wing at C&AG HQ. OIOS should aid in capturing the necessary versions (including the final approved) in the system. The same may be published into the central repository at a later time after seeking approval from competent authority along with the linked Audit design matrix, IT-based audit toolkits and sampling approach document.

21.1 Actors involved

The actors involved in approval of audit guidelines.

- **Designer** proposes the audit guidelines with the relevant design elements.
- **Reviewers** review the guidelines and provides feedback.
- **Approver** approves the guidelines.

21.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Preparation of audit guidelines.
- Linking of audit design matrix.
- Linking of sampling approach.
- Review of audit guidelines.
- Approval of audit guidelines by the competent authority.
- Publishing of audit guidelines after seeking approval of competent authority into the central repository.
- Search for relevant audit guidelines stored in central repository.
- Download relevant audit guidelines.

22 T&M phase of Audit design module

The following functionalities are expected to be taken up during the T&M phase of OIOS project.

22.1 Statistical sampling (05_04)

The technique of statistical sampling is used to select the auditable entities at various levels of auditable entity (See illustration below) and transactions (if electronically available). In the absence of electronic data, the process is manual and only documentation would be attached (as explained in the above sub-module 05_01). The approach to selection may be one of the following.

- Simple random sampling -> with/without replacement
- Judgemental sampling (Should be rarely used with justification)
- Stratified random sampling
- Multi-stage cluster-based sampling
- Probability proportional to size sampling -> monetary unit, weighted combination of different parameters, combination of multiple parameters.
- Others

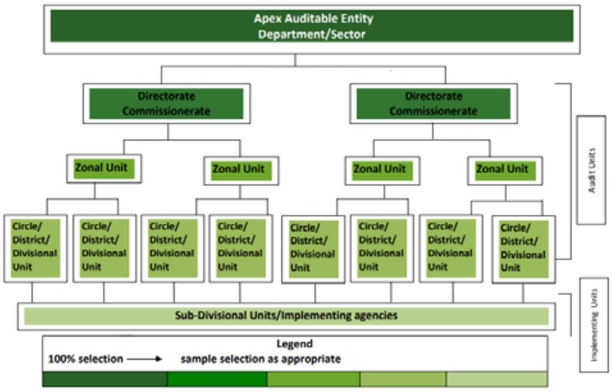

Apex Auditable Entity
Department/Sector
Directorate
Commissionerate
Directorate
Commissionerate
Zonal Unit
Zonal Unit
Zonal Unit
Zonal Unit
Circle/ District/ Divisional Unit
Circle/ District/ Divisional Unit
Circle/ District/ Divisional Unit
Circle/ District/ Divisional Unit
Circle/ District/ Divisional Unit
Circle/ District/ Divisional Unit
Circle/ District/ Divisional Unit
Circle/ District/ Divisional Unit
Sub-Divisional Units/Implementing agencies
Audit Units
Implementing Units
Legend
100% selection
sample selection as appropriate

Figure 4: Illustration of sampling at multiple levels of auditable entity for an audit assignment

06 Audit Execution

This module includes five sub-modules that are related to execution of an individual audit assignment.

- The ‘**Programme**’ sub-module facilitates in managing allocation of personnel to field audit programmes, approval of the tour programme and deviation process (including post facto approval). Upon approval, the sub-module also communicates intimation of the program to the auditable entity.
- The ‘**record requisition**’ sub-module manages the process of requesting and receiving records that are required for audit. It also monitors non-receipt and delay in receipt of records.
- Then, the ‘**audit enquiry**’ sub-module provides a platform to prepare, issue preliminary audit enquiry and receive reply to audit enquiry. These audit enquiries may become converted into an audit observation or dropped based on reply of the auditable entity. Alternatively, the audit team may decide to issue an audit observation directly.
- The preparation and issue of audit observation is facilitated by ‘**Audit observation**’ sub-module. The sub-module also provides for receipt of reply to the observation. The requisition, enquiry and observation modules will also have features for collecting and referencing a variety of supporting documentation in various formats – which may be linked at different points of time (during and after audit execution), some of which may remain unlinked.
- The ‘**audit toolkit (collect)**’ sub-module assists in collecting data that may be necessary for answer an audit question or fulfil an audit objective / sub-objective as part of an ADM-based audit (typically either a Performance Audit or a theme-based/ subject-matter specific Compliance Audit).

23 Audit Programme (06_01)

The responsibility of execution of the audit plan/guideline for each audit assignment is vested with one or more audit teams. One of the members of the team is assigned as the team leader. Some of these teams may also be engaged earlier than audit execution, performing the roles of preparers of audit guidelines. When there are more than one team for a single audit assignment, then one of the teams is also chosen as the ‘nodal’ team for the assignment to facilitate co-ordination of effort and consolidation of outputs.

It is also possible that a single audit team may perform multiple audit assignments in parallel. For example, an audit team for conducting a Performance audit, covering various auditable entities, may, in addition, be tasked with conducting compliance audits of some (or all) of these auditable entities along with the performance audit. This should be reflected through a pop-up during data entry for the second (parallel) assignment, stating that some or all members are also taking up another assignment at the same point of time (or with overlapping timeframes), but not preventing “creation” of such parallel assignments. There should be a cross-reference or link between the assignments where the team leader for multiple assignments is common.

23.1 Creating audit teams

The selection of members for an audit team for a particular assignment is normally, but not always, restricted to the functional wing of a FAO, especially in compliance audit assignments. However, in case of performance audit topics and topics cutting across various functional wings of FAO, the members of the team may be chosen across functional wings of a FAO. In the case of members cutting across functional wings of a FAO, the proposal is initiated by a central co-ordination team or with the approval of a central competent authority (as configured by field audit offices).

In the case of All-India performance audits and performance audits co-ordinated among field audit offices, the audit teams from different FAOs are nominated for the assignment by the respective FAOs. There may be more than one audit teams from a FAO who would be engaged in the All-India PAs. In that case, there would be one nodal team assigned as well. There will be an audit team from the lead FAO, which will be the lead audit team.

23.2 Amending composition of audit teams

The composition of audit teams is subject to modification at any point of time. The system should facilitate additional of new members to the created audit teams, re-designation of audit team leader, removing team members from audit team and re-assigning members to another audit teams. The system should automatically make necessary modifications to the access control.

23.3 Scheduling

Apart from the process of creating/amending audit teams, Audit programming also refers to the process of attaching audit teams to specific auditable entities and scheduling[59] their visit to auditable entities. After the programme is approved, the same is intimated to the auditable entities through digital communication interface or email or through a paper-based letter. It is important to note that an employee can be a part of several audit teams, as we can also have the audit assignments run in parallel. During a scheduled visit to an auditable entity, i.e. a programme, the team member may be carrying out tasks relating to more than one assignment[60]. For example, during a programme of District Educational Officer in the Bilaspur district in Himachal Pradesh, the team member may be carrying out tasks relating to 'All-India Performance audit of Sarva Shiksha Abhiyan scheme' and 'Compliance audit of selected themes/ activities of the District Development Officers'.

The necessity to deviate from the original schedule might arise for various reasons. The deviation is normally requested by the audit team which is then submitted for approval by competent authority. In some cases, the deviation is directed by the competent authority. Deviations may be proposed and approved post facto. The various kinds of deviations are discussed below. These deviations may be approved post-facto by the competent authority.

- **Extensions** arising out of requirement of additional days to complete the audit execution.
- **Pre-closure** arising perhaps out of excess allocation of days in original schedule.
- The audit schedule may be **suspended** temporarily due to diversion of audit team to another schedule and **resumed** after the completion of diversion.
- The audit schedule may be **cancelled** due to various reasons.

[59] In regard to scheduling, the working calendar (in relation to field audit teams) varies for each of the field audit office and sometimes for each of the functional wings of FAO. This is because, the field audit teams visit the auditable entities based on their working calendar which may vary because of the different holidays in the state level and the local level and also because the auditable entity might be working additional days. It is also important to note that the working calendar for the field HQ also varies for each field audit office. However, within a field audit office, it remains the same for HQ sections of the wing concerned.
[60] There exists a many-to-many relationship between audit programmes and audit assignment/sub-assignment.

- The schedule may also be **deferred/postponed** to another point in time.

Indicative business data relating to audit programme

- For each assignment,
  - Audit team reference number
  - Which are the audit teams?
  - Who are the members of the audit teams?
  - For each member,
    - Date of start of membership
    - Date of end of membership
- For each audit team in each assignment
  - List of auditable entities to be visited by them
  - Original dates of visit
  - Actual dates of visit (the original and actual dates will differ based on deviation, if any)
  - Deviation requests
- For each deviation request,
  - Who requested it?
  - Date of requisition
  - Nature of deviation (Extension, Pre-closure, Suspension, Resumption, Cancellation, Deferral)
  - Remarks relating to request
  - Status of request (Approved / Denied)
  - Date of approval/denial
  - Remarks of approver
- For each programme, the following audit documentation will be captured as attachments,
  - Allocation of work by team leader to the members of the team (for audits making use of toolkits, the allocation should specify the allocation of toolkits to members of the team)
  - Entry meeting minutes
  - Daily work diary
  - Exit meeting minutes
  - Title sheet / Top sheet (In the form of a check list or attachment)
  - Code of ethics

23.4 Activities that are typically undertaken during a programme

The following are the list of activities that are undertaken typically during a programme.

- **Entry meeting:** The process of meeting is outside the scope of OIOS. The minutes of the meeting is captured as an attachment of the programme
- **Allocation of work:** The allocation of work is captured as a to-do list (as described in the subsequent sections) for each of the member of audit team member.
- Requisition and receipt of records as detailed in the sub-modules subsequently (06_02).
- Preparation, issue of audit enquiries, receipt of response and processing of audit enquiries as detailed in the sub-modules subsequently (06_03).
- Preparation, issue of audit observations, receipt of response and processing of audit observations as detailed in the sub-modules subsequently (06_04).

- Miscellaneous tasks as captured in allocation of work, where the documentation of tasks is captured as attachments to the programme.
- Filling up of the digital diary (as described in the subsequent sections).
- Uploading and processing of replies received for outstanding observations from previous inspection reports (as described in the subsequent sections).
- Scanning of key documents (as described in the subsequent sections).
- Uploading of key documents (as described in the subsequent sections).
- Linking of key documents (as described in the subsequent sections).
- Preparation of draft inspection report (covered in Module 07: Audit reporting
- **Exit meeting:** The process of meeting is outside the scope of OIOS. The minutes of the meeting is captured as an attachment of the programme.

23.5 To-do list of a programme

The to-do list of a programme contains specific list of activities that are to be taken up during the audit programme by each audit team member. This to-do list is prepared in the following manner.

a) The list of activities to be done is listed by the team leader. The team leader allocates the activity to team members.
b) The list of activities to be done is filled by the field headquarters. For example, verification of a complaint or RTI, specific observations to be noted, specific issues to be audited in addition to the original scope, verification of action taken by the auditable entity, etc. The team leader upon receipt of such additional work, then allocates the activity to the team members.

23.6 Digital diary of a team member

The digital diary of team member will list the activities from the to-do list that have been allocated to the member. The team member can choose to update the status on the same. Apart from the above, a summary of activities performed by the member in the OIOS system, such as, issue and processing of audit requisition, audit enquiry and audit observations is also readily available. The digital diary of a team member can be viewed by the team leader and the Group officer.

23.7 Uploading and processing of replies received for outstanding observations from previous inspection reports

The audit team may receive replies for the outstanding observations (observations which are still pending) during the field audit programme. The members of the audit team must be able to invoke the '**09: Communication**' module followed by '08: Audit follow-up' module in order to process the replies received by them.

23.8 Uploading of Key Documents

The records collected by the field audit team which form part of audit documentation and audit evidence are referred to as 'Key documents'. These documents (in any language) may be in digital or paper form. In case of the documents being in paper form, the same would be scanned by the audit team members using mobile app of OIOS (as described in the sub-module (06_06) subsequently) or by other means. The scanned document will then be uploaded into OIOS.

During the upload of key documents (scanned files, photos, videos, etc.,), the system needs to verify whether the documents satisfy the minimum technical specifications. The key documents can be uploaded directly to the programme. OIOS should allow linking of the uploaded KDs to an audit requisition or audit enquiry or audit observation at a later stage. In some cases, the key documents may also be uploaded and linked immediately. Further, there might be key documents which remain unlinked, but are available for reference. There will also be cases, where the key documents (being voluminous) are not uploaded or uploaded only partly, but will remain available in paper form, to be uploaded on an “as-needed” basis.

While uploading Key documents on the OIOS system, the audit team will define the security classification of the documents as Unrestricted/Restricted/Confidential/Secret, if and wherever necessary. The access to key documents will be based on the security classification. The key documents marked as ‘Secret’, if uploaded, shall be stored in the system in encrypted form in the OIOS repository using the encryption keys. The encryption keys shall be stored in Hardware Security Module (HSM).

23.9 Linking key documents

As explained before, the key documents could be either uploaded to programme without specific linking or specifically linked to an audit requisition, or audit enquiry or audit observation. While linking the rich text fields of the audit requisition, audit enquiry and audit observation, OIOS should allow the user to link to entire document or link to one or more specific highlighted (in case of text) or selected area (in case of scanned image) sections of the document.

23.10 Actors involved

The following actors are involved in the process of audit programming (iterations of draft audit programmes will not be captured).

Creation of audit teams for each audit assignment

- **Initiator** proposes the audit teams and their composition/membership for each assignment.
- **Reviewers** reviews and provides feedback on the proposed audit teams and their membership.
- **Approver** approves the proposal.

Scheduling or preparation of audit programme

- **Initiator** proposes the allocation of auditable entities to an audit team and the schedule.
- **Reviewers** reviews and provides feedback.
- **Approver** approves the proposal.

Deviation of programme

- **Employees as members of audit teams/ other competent authority** initiate proposal for deviation
- **Approver** reviews and approves the deviation proposal. Sometimes, the deviations are directed by the approver.

23.11 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Initiate proposal for nomination of audit teams for each assignment.
- Review proposal for nomination of audit teams for each assignment.

- Approve proposal for nomination of audit teams for each assignment.
- Send notification to the nominated members after approval.
- Initiate proposal for audit programme.
- Review proposal for audit programme.
- Approve proposal for audit programme. Send notification to the auditable entity.
- Initiate deviation proposal.
- Review deviation proposal.
- Approve deviation proposal. Send notification to the auditable entity.
- Direct a deviation. Send notification to audit team members and the auditable entity.

24 Record requisition (06_02)

A fundamental requirement for the audit teams to execute the audit plan is access to the relevant set of documents, records and electronic data of the auditable entity. They are, in total, referred to as 'records'. While some of the records would be available to the audit team beforehand, they are generally used in audit planning and design. During the execution at the field, the necessary records would be requested through a formal communication process. OIOS would provide for initiating a request for a record to the auditable entity either through a traditional paper-based format or through a digital communication interface. In the case of traditional format, the audit requisition is printed, signed and handed over to the auditable entity.

If the auditable entity had registered as a temporary user for the audit programme, then the same would be available in the inbox. In the case of API based digital interface, the auditable entity would receive the requisition in the inbox of the IT application of the auditable entity. After receiving the request for the record, the auditable entity may submit the relevant records in traditional paper-based format or through a digital communication interface (either API or temporary userid). If the records are received through the digital communication interface, it is automatically loaded and notification is sent to the audit team who requested it.

However, if the records are received through the traditional mechanism, then the audit team scans and attaches the relevant pages or uploads the electronic data, wherever necessary. This is because some of the records such as service books, manual registers, etc., cannot be completely scanned. Therefore, in such cases, the audit team manually marks it 'received' (fully or partially) and enters the date of receipt in the system. The audit team can request for multiple items / records in the same requisition. In that case, the receipt of records needs to be tracked item-wise (Many to many[61] relationship). OIOS will be able to provide BI on the time taken for responding to audit requisitions, delay/ non-provision of records etc.

Indicative business data relating to record requisition

- Requisition reference number (auto-generated)
- Who requested it?
- Date of requisition
- Subject
- Detailed request (Rich text editor with Hindi typing)

[61] One response can contain response to many audit requisitions. The records requested may be received in phases through various responses.

- Annexure to request (list of items)
- Attachments during request, if any
- Expected date of receipt of record
- For each item in the list,
    - Has the record been received?
    - Quality of records received (Fully or partially received)
    - Additional remarks
    - If yes, Actual date of receipt of record
    - Attachments related to records received, if any

24.1 Actors involved

The following actors are involved in the process of Change management (Process).

- **Team members** initiates an audit requisition.
- **Auditable entity (external)** receives and provides responses (records) to the audit enquiry.

24.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Request for record.
- Receipt of record (Digital communication interface).
- Scanning and uploading of received record (traditional channels)

25 Audit Enquiry (06_03)

This is an optional sub-module, where the members of the audit team prefer to issue a preliminary audit enquiry to elicit the preliminary response of the auditable entity before finalising the audit observation. The audit team peruses the records produced to them and/or test checks of the selected sample of transactions and decides to issue an audit enquiry first. The audit enquiry may mature into an audit observation based on the response of the auditable entity or otherwise. When the team member decides to prepare an observation, the system should allow to copy the contents of the audit enquiry to the audit observation, which would be modified thereafter. Many audit enquiries may be clubbed into an audit observation. One audit enquiry can result in multiple audit observations, or parts thereof, as well.

The audit enquiry (after approval of team leader) is communicated through a formal communication process. OIOS would provide for communicating the audit enquiry to the auditable entity either through traditional paper-based format or through a digital communication interface. If the response to the audit enquiry is received through the digital communication interface, it is automatically loaded and notification is sent to the audit team who issued the audit enquiry. However, if the response is received through traditional mechanism, then the audit team scans and attaches the response. Then, the member of the audit team decides to whether to issue an audit observation or not pursue the enquiry further.

Indicative business data relating to audit enquiry

- Audit enquiry reference number (auto-generated)
- Who originated the enquiry?
- Date of origin of the enquiry

- Detailed description of enquiry (Rich text editor with Hindi or other language typing[62])
- Date of approval of the enquiry (wherever applicable)
- Date of issue of the enquiry
- Who issued it?
- Expected date of reply
- Attachments relating to the enquiry
- In case of receipt of reply from the auditable entity
  - Who responded?
  - Date of reply
  - Nature of reply (interim / final)
  - Detail of reply
  - Attachment relating to the reply
  - What is the decision of audit team (Not pursue enquiry further / issue an audit observation)?
  - Remarks relating to decision
  - Who made the decision?
  - Date of decision
  - Reference from audit observation to audit enquiry

25.1 Actors involved

The following actors are involved in the process of issue of an audit enquiry.

- **Team member** initiates an audit enquiry.
- **Team leader** reviews and approves/returns an audit enquiry. The leader can also initiate audit enquiry.
- **Auditable entity (external)** receives and provides responses to the audit enquiry.

25.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Prepare an audit enquiry.
- Review an audit enquiry.
- Approve/return an audit enquiry. Notify the team member who originated the audit enquiry. (if the SOP provides for approval of audit enquiries by the Team Leader)
- Issue an audit enquiry.
- Receive reply (digital communication interface). Notification sent to audit team.
- Receive reply (traditional channel) and scan and upload the same.
- Process reply and communicate the decision to the auditable entity.
- Monitor record request progress

[62] The typing should be similar to Google typing tool. For example, when the user types Namaste, the input tool gives various Hindi words with the most probable one (नमस्ते) in the top.

26 Audit observation (06_04)

The audit team after scrutiny of records produced to them prepares audit observation(s) and issues them to the auditable entity. It is important to note that an audit observation does not necessarily only mean ‘**an adverse finding**’. An audit observation may arise directly out of scrutiny of records and/or test checking of selected sample of transactions. Alternatively, an audit team may choose to issue one or more audit enquiries and then issue one or more audit observations after analysing the responses of the auditable entity, if any. As explained in the previous section, there is a many-to-many relationship between an audit enquiry and an audit observation. An audit observation essentially has four parts including the attachments.

a) **Meta-data (optional):** This refers to the configurable meta-data that an audit team wants to capture in relation to the assignment. OIOS should provide the flexibility of storing templates of such a configuration, which could be reused by audit teams of an audit assignment. An illustrative meta-data template is detailed below. The template is related to an assignment dealing with audit of *implementation of bridge works by Public Works Department*. This is especially useful for compliance audits which are not ADM driven. In case of ADM driven audits, the same can be implemented through one or more audit tool kits.

b) **Audit observation:** This refers to the detailed text containing the actual observation. After drafting the observation, the preparer of the observation also includes references in the text for relevant key documents/ supporting documentation.

c) **Multiple sub-paragraphs relating to the observation (optional):** Each audit observations might have sub-paragraphs within them. For example, during the test check of sampled transactions, the audit team might unearth a common observation. In such cases, the relevant transactions are listed as sub-paragraphs in the audit observation. Such type of listing of transactions also facilitates handling a situation, where the auditable entity has the tendency to respond transaction-wise. One such example would be, list of documents pertaining to an audit observation on ‘*short levy of stamp duty due to misclassification of documents*’, where the documents may be listed as sub-paragraphs.

d) **Attachments:** The attachments for an audit observation would include key documentary evidence (documents which form part of evidence), working sheets or calculation sheets, annexures, etc. The key documents may be electronic documents (Word, Pdf, and Excel), photographs, videos, data files, scanned documents, etc. The attachment also includes criteria (For example, Section xxx of xxx Act), where the attachment would be to the source of the criteria. The necessary for bookmarking (i.e., linking to a specific section in the document) may be considered. Meta-data will be required for attachments (e.g. category, sub-category, title of attachment, key word(s) etc.)

e) **Self-check-list**: The preparer of the audit observation is provided with a check-list (which should be configurable by the office/ wing administrator), which he will fill for every audit observation assuring its quality. For example,

- Has the criteria been clearly defined in the observation?
- Have the conditions been clearly detailed in the observation?
- Has the cause of deviation/non-compliance, if any, been identified?
- Has the effect of deviation/non-compliance, if any been ascertained?
- Have all the necessary documents been attached?

- Was the reply of the head of the office considered before finalisation of the audit observation?

Sample header for audit observations in implementation of bridge works by Public Works Department

- Work Order Number
- Work order value
- Date of issue of order
- Expected date of completion
- Status of the work
- Actual date of completion

Indicative business data relating to audit observation

- Audit observation reference number (auto-generated)
- Who originated the observation?
- Date of origin of the observation
- Detailed description of observation (Rich text editor with Hindi typing)
- Materiality of the observation (High, Medium, Low) and Nature of materiality (by value of financial impact, by context, fraud, social, environmental, etc.)
- Quantity of financial impact, if any
- Link to classification schema. The same paragraph may be classified to one or more categories/sub-categories in one or more schema.
- Date of approval of the observation (wherever applicable)
- Date of issue of the observation
- Who issued it?
- Expected date of reply
- Link the observation to Audit Design Matrix/Audit Tool kit[63] (This will facilitate generation of audit finding matrix)
- Sub-paragraphs and their details
- Attachments relating to the observation
- Is the observation based on one or more audit enquiries?
- If yes, what are the related audit enquires?
- In case of receipt of reply from the auditable entity
  - Who responded?
  - Date of reply
  - Nature of reply (interim / final)
  - Whether the reply relates only a few of sub-paragraphs listed in the observation?
  - If yes, for each sub-paragraph in the reply,
    - Whether the auditable entity accepted the audit observation (accepted / partially accepted / not accepted)?
    - Detail of reply
    - Attachment relating to the reply

[63] There is a many-to-many relationship between audit observations and audit tool kit. One audit observation may be based on answers/data collected in many tool kits. One audit tool kit may be referred in many audit observations.

    - Does the audit team agree with the reply of auditable entity (reply is acceptable / reply is not acceptable / reply requires reconsideration)?
    - What is the decision of audit team (Not pursue observation further / reiterate or update an audit observation)?
    - Remarks relating to decision
    - Who made the decision?
    - Date of decision
  - If no, for the audit observation as a whole,
    - Whether the auditable entity accepted the audit observation (accepted / partially accepted / not accepted)?
    - Detail of reply
    - Attachment relating to the reply
    - Does the audit team agree with the reply of auditable entity (reply is acceptable / reply is not acceptable / reply requires reconsideration)?
    - What is the decision of audit team (Not pursue observation further / reiterate or update an audit observation / required action has been taken by the Department)?
    - Remarks relating to decision
    - Who made the decision?
    - Date of decision

26.1 Actors involved

The following actors are involved in the process of issue of an audit observation.

- **Team member** initiates an audit observation.
- **Team leader** reviews and approves/returns an audit observation. The leader can also initiate audit observation.
- **Auditable entity (external)** receives and responses to the audit observation.

26.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Prepare an audit observation.
- Review an audit observation and propose necessary changes.
- Approve/return an audit observation. Notify the team member who originated the audit observation (if the SOP provides for review and approval of the audit observation by the team leader).
- Issue an audit observation.
- Receive reply (digital communication interface). Notification sent to audit team.
- Receive reply (traditional channel) and scan and upload the same.
- Process reply and communicate the decision to the auditable entity.
- Monitor execution progress

27 Audit Toolkit (Collect) platform (06_05)

This sub-module assists in collection of data in the audit tool kits. The audit-tool kits that were created by the designer as part of the audit guideline process is available for the team members to fill in. After the completion of audit execution of a programme in an auditable entity (or even during), the team members collect audit findings/ data in the tool kit. The team members, also receive a notification, if the design of the audit tool kits were changed in the interim.

In case of audit checklists, the audit team member must be able to upload a list of transactions (txt, csv, Excel) that were selected after risk assessment and then execute the checklist against each one of the transactions.

27.1 Actors involved

The following actors are involved in the process of audit toolkit (collect) are the following.

Audit team members collect audit findings/ data using the toolkit.

27.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Collection of data through toolkit.
- Submission of data through toolkit.
- Re-collection of data through toolkit, in case of change in design or other reasons.

28 Offline utility (06_07)

The audit execution module would be used by many of the employees of the Department as audit execution is the most crucial part of the audit assignment. Audit execution is mostly conducted in the premises of the auditable entity. Hence, the employees using this module would be geographically distributed and constantly mobile. The quality of internet connectivity in the premises of the auditable entity / geography varies. Hence, it is important for this module to switch from online mode to offline mode (as a backup) based on availability of internet connectivity. That is, if the internet connectivity is not available, then the module should work on an 'offline' mode where the data created by individual team members are stored locally. Upon the internet connectivity being available, the module should "auto-sync" the data to the global server, which is then available for continuous workflow. It is important to note that this is only being conceived as a 'backup' solution (should be made as 'light' as possible) and efforts would be made to find alternate solution (in collaboration with SI) for a better solution. It is also expected that with continuous improvements in availability of Internet connectivity in field locations throughout India, the need for offline mode will decrease with time.

Offline functionality is NOT required for connectivity in the Headquarters locations of the Field Audit Offices, only for the field audit teams.

One simple way to handle this would be to have the offline functionality as part of mobile app alone. The users can install the mobile app on top of emulators of mobile operating system (such as Android, iOS, etc.) in their laptop in order to use the big monitor screen of laptop. At the same time, this approach relieves IA&AD from maintain both stand alone and web versions of the same product. Another way to handle this is to have centrally driven offline application, which can be downloaded from the OIOS application and installed (and updates pushed automatically when the audit team member logs into OIOS) [64] by the audit team member.

The following functionalities are expected to be in the 'offline' mode.

1) Access to documents in KMS, which were chosen to be 'Make available offline' in advance by the user.
2) Collection of data using the kit.
3) Preparation of audit requisitions, audit enquiries and audit observations (which will be printed, signed and issued to auditable entity).
4) Queue up scanned documents for uploading.
5) Attach/ Link replies and attachments to audit requisitions, audit enquiries and audit observations. (subject to technical feasibility)[65]

Upon availability of the internet, the need for updates of utility and syncing of the data must be ascertained and automatic update and syncing of the data must be done. If the system identifies any data discrepancy, the same must be highlighted to team member so that it can be resolved.

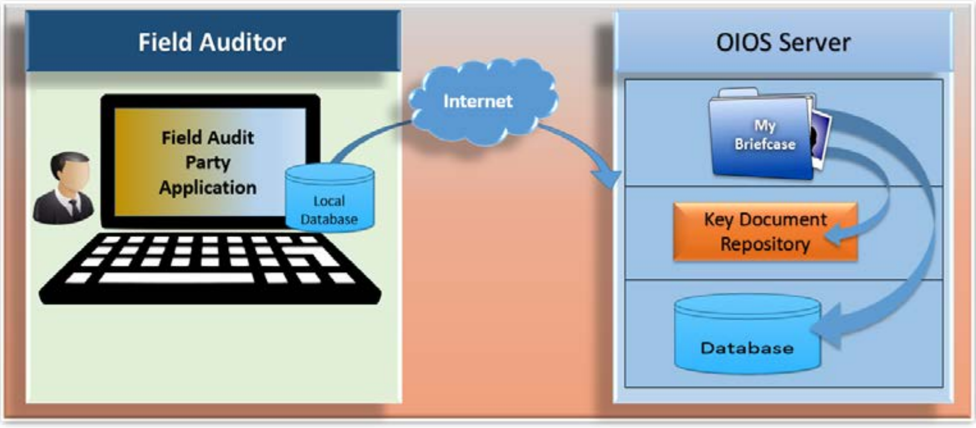


Figure 5 Offline/Online switching of module

28.1 Scanning of documents

As described in the earlier sections, the field audit members have the necessity to scan and upload documents during several occasions and link them in the audit execution module. OIOS would provide for a mobile application to scan the documents and store internally and then upload the same to the OIOS server. The documents will then be attached in the OIOS ecosystem to the relevant entities. The same application can also be used to capture photographs and / or videos. The photographs, videos and scanned documents must have a real-time date and timestamp, geographical location, IMEI, etc. OIOS should provide for authentication of the scanned documents, photos and videos by basic physical signature of the person from auditable entity (Digital signature is not required).

The minimum specifications for scanning, photos and videos need to be specified so that there is assurance in minimum quality. The solution should allow for scanning multiple pages in the same

[64] The installation must be a very simple process. The audit team member should be able to install without any configurations.

[65] The last functionality of attaching/ linking is subject to technical feasibility involved in a very light offline app. If this is not technically feasible, such attaching/ linking can be done later when online.

document. After scanning, the solution must provide a preview of the page, so that the team member can verify quality in terms of readability. The system should provide the option to improve brightness, sharpness and contrast of the scanned image of the page to improve readability, if necessary.

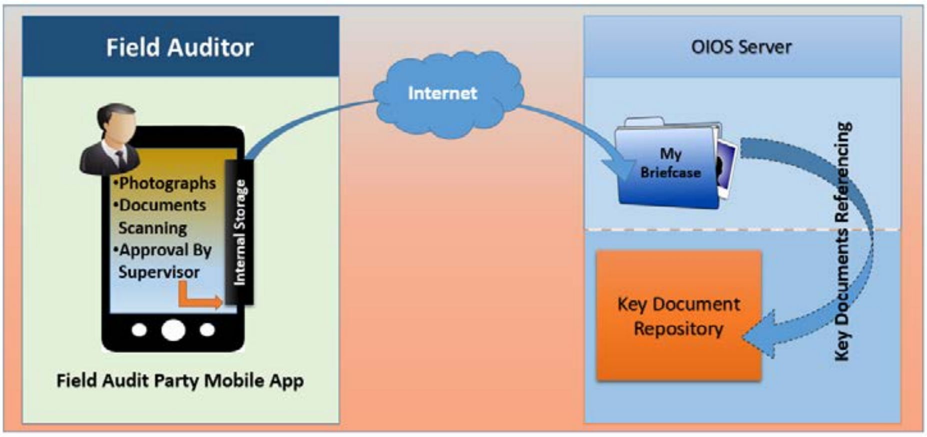


Figure 6 Scanning of documents during audit execution

29 T&M phase of Audit execution module

The following sub-modules are envisaged in the Time & Material phase of implementation.

29.1 API Integration with auditable entities (06_06)

The audit teams of field audit offices communicate audit intimations, audit requisitions, audit enquiries and audit observations to the auditable entities during the audit execution stage. The audit teams also receive acknowledgement, responses to audit requisitions, audit enquiries and audit observations from the auditable entities during the audit execution stage. This communication is envisaged to happen through an API-based communication interface between IA&AD and auditable entities.

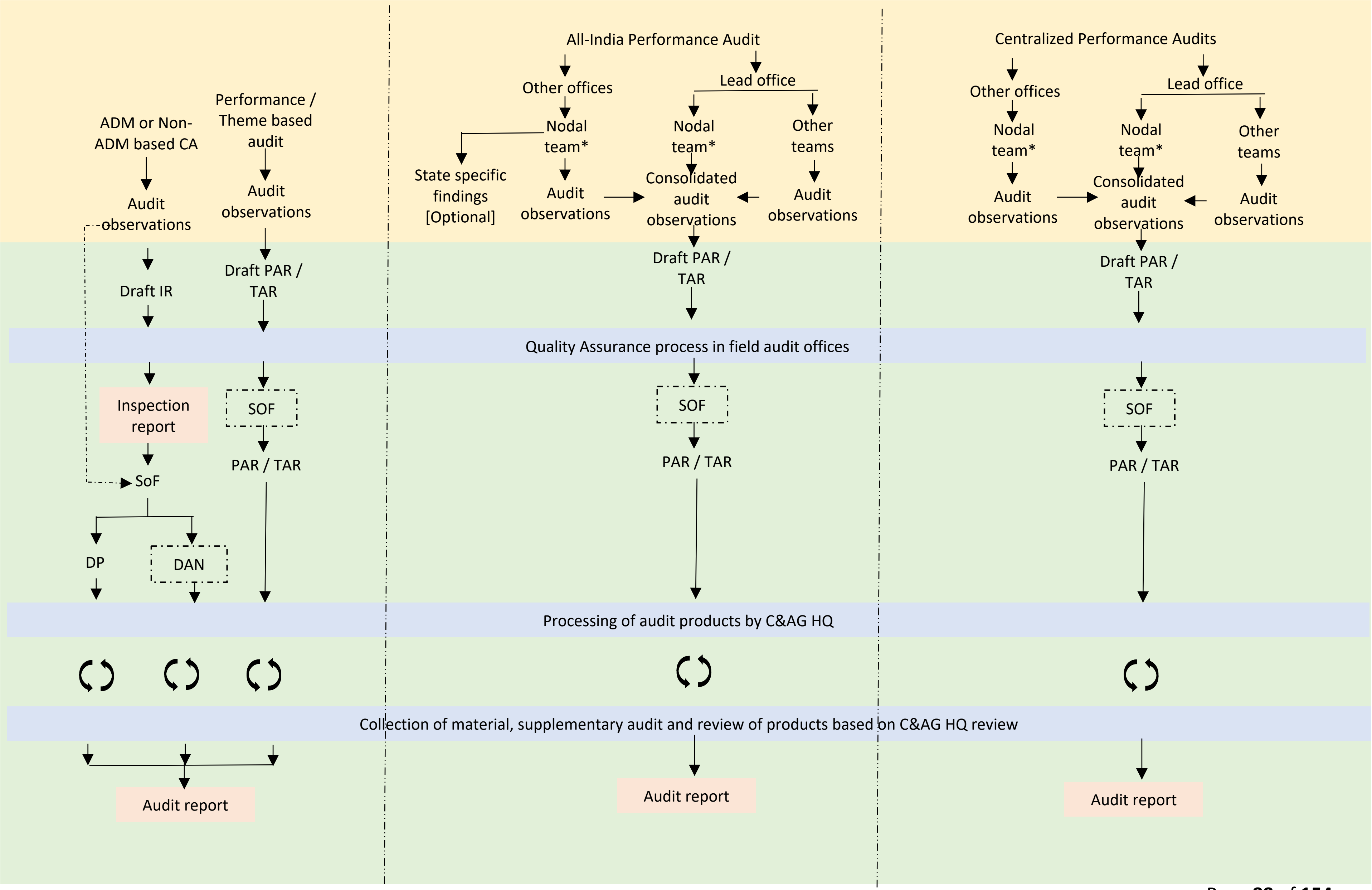
Since the number of auditable entities are large, the most efficient way to handle this API interface is as an interface between IFMS (Integrated Financial Management Systems) of the State/UT Government and PFMS (Union Government). OIOS project envisages establishing these interfaces in the future phases. The implementation of these interfaces will be staggered and are based on readiness of the IFMS and PFMS systems. Hence, this sub-module is proposed to be implemented as part of future phases.

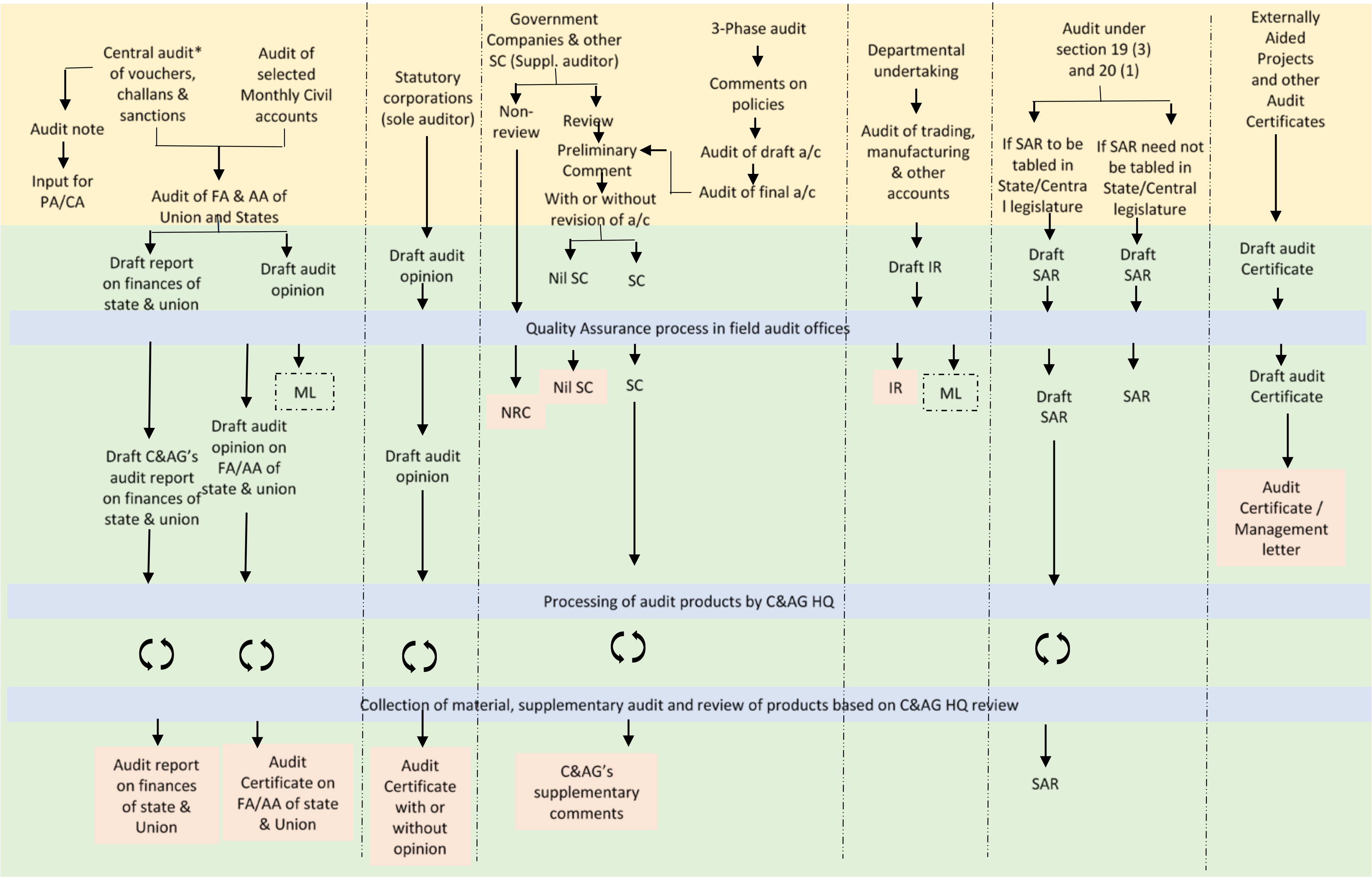
07 Audit Reporting

After the completion of audit execution as per the plan, IA&AD reports the findings and observations in various audit products. This module provides a platform to prepare draft audit products, to conduct quality control or provide quality assurance to an audit product. It would also aid in finalising, issuing / communicating the products to relevant stakeholders and receiving their response. Some examples of audit products are Inspection reports, Statement of Facts, Draft Paragraphs, Departmental Appreciation Note, Management Letter, C&AG's Audit Report, Audit certificates, Separate audit reports and C&AG's supplementary comments.

30 Configuration of Audit products (07_01)

The process of preparation and issue of the products is illustrated in the diagram below. The section shaded in yellow represents the 'Audit execution' which precedes the 'Audit reporting' process (represented by the green section).


ADM or Non-ADM based CA
Audit observations
Draft IR
Inspection report
SoF
DP
DAN
Performance / Theme based audit
Audit observations
Draft PAR / TAR
SOF
PAR / TAR
All-India Performance Audit
Other offices
Nodal team*
State specific findings [Optional]
Audit observations
Lead office
Nodal team*
Other teams
Consolidated audit observations
Audit observations
Draft PAR / TAR
SOF
PAR / TAR
Centralized Performance Audits
Other offices
Nodal team*
Audit observations
Lead office
Nodal team*
Other teams
Consolidated audit observations
Audit observations
Draft PAR / TAR
SOF
PAR / TAR
Quality Assurance process in field audit offices
Processing of audit products by C&AG HQ
Collection of material, supplementary audit and review of products based on C&AG HQ review
Audit report
Audit report
Audit report


Central audit* of vouchers, challans & sanctions
Audit of selected Monthly Civil accounts
Audit note
Input for PA/CA
Audit of FA & AA of Union and States
Draft report on finances of state & union
Draft audit opinion
ML
Draft C&AG's audit report on finances of state & union
Draft audit opinion on FA/AA of state & union
Audit report on finances of state & Union
Audit Certificate on FA/AA of state & Union
Statutory corporations (sole auditor)
Draft audit opinion
Draft audit opinion
Audit Certificate with or without opinion
Government Companies & other SC (Suppl. auditor)
Non-review
Review
Preliminary Comment
With or without revision of a/c
Nil SC
SC
NRC
Nil SC
SC
C&AG's supplementary comments
3-Phase audit
Comments on policies
Audit of draft a/c
Audit of final a/c
Departmental undertaking
Audit of trading, manufacturing & other accounts
Draft IR
IR
ML
Audit under section 19 (3) and 20 (1)
If SAR to be tabled in State/Centra l legislature
If SAR need not be tabled in State/Central legislature
Draft SAR
Draft SAR
Draft SAR
SAR
SAR
Externally Aided Projects and other Audit Certificates
Draft audit Certificate
Draft audit Certificate
Audit Certificate / Management letter
Quality Assurance process in field audit offices
Processing of audit products by C&AG HQ
Collection of material, supplementary audit and review of products based on C&AG HQ review

*Note: The procedure varies between Union and State Government accounts

Figure 7: Audit products in C&AG (Part 2)

*Note: Procedure varies between audit of Central and State Government accounts

As detailed in the illustration, some audit products are issued after processing of the material by C&AG HQ and others are directly issued by the field audit office. The complete list of audit products varies from one field audit office to another. The most common audit products of IA&AD are briefly described below.

30.1 Audit products issued in IA&AD

The following are the most common audit products issued in IA&AD.

a) **Draft Inspection report (DIR):** This is the draft stage of inspection report which is prepared by the audit team after finalising the audit observations. This is formally discussed with the head of the auditable entity just during the exit meeting, to elicit their response. The same is forwarded to the Quality assurance team in the headquarters of field audit offices.

b) **Inspection Reports (IRs):** These reports are issued by the field audit offices after the completion of compliance audit of specific auditable entities. The draft IRs undergo a QC/QA process in the field audit offices. They are not subjected to processing by C&AG HQ. The audit observations in inspection reports are pursued by the respective functional wings of a FAO in the field audit offices as explained in the '**08 Audit follow-up**' module.

c) **Draft PAR/TAR:** This is the draft stage of performance and theme-based compliance audit reports which is prepared by the audit team after finalising the audit observations, wherever necessary. This is issued as a consolidated finding report to the relevant apex auditable entities (optional).

d) **Statement of Fact (SOF):** The statement of fact is the first level of communication to the Government[66] with an endorsement to the auditable entities regarding inclusion of the specific set of audit observations in the final audit report to be placed in the State/Central legislature. This product is optional in performance or thematic audits.

e) **Draft paragraph (DP):** The Draft paragraph represents the communication from the head of the field audit office to the Government with an endorsement to the apex auditable entities (where different). The communication is regarding possible inclusion of the specific set of audit observations in the final audit report to be placed in the State/Central legislature. As an alternate to DP, which typically represents a specific type of observation, a holistic Departmental appreciation note can also be made by the field audit office.

f) **Departmental appreciation note (DAN):** In the case of ADM based Compliance audit, the field audit office may opt for preparation of a Departmental Appreciation Note as a whole. This is alternate to a string of DPs, which serves as an assortment of individual audit observations. The DAN provides a holistic view of the subject matter handled in the compliance audit assignment. It is communicated by the head of the field audit office to the Government with an endorsement to the auditable entities. The communication could be regarding possible inclusion of the DAN as a holistic compliance audit report on the specific subject matter in the final audit report to be placed in the State/Central legislature. The DAN may be directly prepared from the IRs issued for the compliance audit or there can be an interim SOF as well.

g) **C&AG's Audit Reports:** These reports are typically signed by the head of the field audit office[67] after processing at C&AG HQ and approval by the C&AG of India, who countersigns the Audit Reports. These reports include reports containing significant findings of compliance audits and

[66] Government means the Department or Ministry, rather than an attached or sub-ordinate office of the Government.

[67] Some Audit Reports (e.g. Union Audit Reports on Central Revenues, PSUs etc.) may be signed by an officer at Headquarters Office.

performance and theme-based audits. The findings on finances of States / Union are issued as a separate report. Sometimes, individual Performance Audits may be issued as “Stand-alone” Reports. The organisation of contents of individual reports varies a lot. They may be organised sector-wise or for a state as a whole or for specific audit streams of Union Government, etc. Therefore, the organisational hierarchy for the processing of material to be included in the audit reports and hence the workflow also varies. These reports are tabled in Parliament/ State Legislature and stand referred to the respective committees of Parliament/ Legislature (Union/State/UT). The placement of the reports in Parliament/ State Legislature[68] is covered in this module, but its follow-up mechanism has been discussed in ‘**08 Audit follow-up**’ module.

h) **Draft SAR/SAR:** The Separate Audit Reports are issued on the financial statements of auditable entities whose mandate falls under Section 19(3) and 20(1). If the SARs are to be tabled in the legislature, then it is subjected to processing by C&AG HQ. Otherwise, the SARs are issued after QA/QC within the field audit offices.

i) **Audit Reports on Autonomous District Councils (ADCs) are approved by the C&AG and submitted to the Governor for being tabled in the Council.**

j) **Draft audit opinions/comments:** This is the draft stage of audit opinion or comments or supplementary comments as part of financial attest audits of accounts of auditable entities. These comments are communicated to the auditable entities. The auditable entities may subsequently revise their accounts based on the draft comments. Some variations are Non-Review Certificate (NRC), Nil Comments (NC), Supplementary Comments (SC), etc.

k) **Audit certificates:** Audit certificates are audit products of other financial attest audits. While, the processing of the material relating to audit certificate is detailed in the previous section. This section deals with maintaining information about the Audit Certificate which are issued after approval of C&AG HQ.

l) **Management letter (ML):** A management letter is an audit communication product from the head of the field audit office to the relevant apex auditable entities and/or Government. ML is a means to communicate and draw attention of the decision makers to specific systemic issues which require special attention. In most cases, it arises out of observations from one or more assignments. They may also a supplement to financial attest audit opinion or comment or certificate. However, explicit linkage to audit observations need not be maintained.

m) **Other Audit Products:** Apart from the products described in the preceding sections, there might be other local audit products issued by the field audit offices. For example, audit notes, pilot audit report, data collection reports, press brief, epitome, bond copy, suo-motu correction, etc.

Apart from the original audit product, the system should also assist in preparing and issuing supplementary products to the original audit product and errata to original audit product. The linkages between audit observations with Audit products (say Inspection report) and between audit products (say SOF and DP; DP and IR; DP and AR, etc.) should be traceable.

[68] It is necessary to capture the date of placement of the C&AG’s Audit Report in Parliament/ State Legislature as the case may be.

30.2 How would these audit products be envisaged in OIOS?

In OIOS, all the audit products would be essentially envisaged as document types in a document management system. Then for each audit product, the administrators needs to perform the following once.

a) Configuration of business data.
b) Configuration of workflow.
c) Configuration of ranking parameters, where needed.

The above configurations can be stored as a template to be reused across field audit offices. Apart from the above, OIOS should provide facility to configure and set up a 'Shabdhkosh[69]' to facilitate multi-language search.

30.2.1 Configuration of business data

The business data relating to the audit products cannot be completely standardised. However, there are certain common data fields for all the audit products which would be maintained in OIOS. Further, OIOS would provide the facility to configure specific fields for specific document types which is common across field audit offices. Apart from this, the field audit offices may also want to maintain special fields for specific audit products. OIOS would provide a facility to configure these special fields as well. However, the configuration would be reviewed by the application administrator before approval of the competent authority. Thus, there are three different configurations that are required.

a) Business data that are common across all audit products and all field audit offices.
b) Business data that are specific for each product but common for all field audit offices.
c) Business data that are specific for each product and specific for a field audit office.
d) Business data that are specific to a group of field audit offices belonging to one audit stream.

The indicative business data that are common across all audit products and all field audit offices is detailed below.

Indicative business data that are common across all audit products and all field audit offices

a) **Meta-data (common):**
What is the communication reference number?
Who issued it?
When was it issued?
Whom were it issued to? (May be endorsed to more than one recipient)
By when a response was expected?
Link to assignment/sub-assignment in annual audit plan, if applicable

b) **Product change history:**
Who made the change?
When was the change made?
A short description of the changes made.
Status change, if any.
What is the version number?
Content of the product

c) **Product (versions):** This refers to the changed versions of the product while it undergoes quality assurance or review. Each version contains the actual content of

[69] 'Shabdhkosh' is audit dictionary with equivalent words in English, Hindi and other languages.

the product. The content of the product is hyperlinked to Product key and key documentary evidence, in relevant paragraphs and sections. OIOS should facilitate storing versions which were not generated as a result of workflow in OIOS.

d) **Attachments:** Any attachments relating to the product such as annexures, etc. would also be stored by OIOS. However, the attachment types configurable for each product.

The business data that is configurable in the OIOS for each product type is listed below.

a) **Meta-data (additional):** This refers to the configurable meta-data that a field audit office wants to capture in relation to the product. OIOS should provide the flexibility of storing meta-data templates as a configuration, which could be shared and used by the field audit office.

b) **Product Key:** Configurable for each product

30.2.1.1 Configuration of additional meta-data for each product type

As detailed earlier, each product may also have additional meta-data fields which are not standardised or uniform. An illustrative list is enumerated below.

Product	**Illustrative list of additional meta-data fields**
Inspection report	Status (Under preparation/ under review/issued/closed) Is it a supplementary report? If yes, to which report is it supplementary to?
Statement of Fact	Status of SOF (under preparation/under review/issued/received response/open/not pursued further/Converted into DP)
Draft paragraph	Status of DP (under preparation/under review/issued/received response/open/not pursued further/Communicated to HQ/under process by HQ/deferred by HQ/dropped by HQ/featured in Audit report) Note: Some of the statuses are result of processing of DP by HQ which is covered in the subsequent section.
Departmental appreciation note	Status of DAN (under preparation/under review/issued/received response/ /Communicated to HQ/under process by HQ/featured in Audit report) Note: Some of the statuses are result of processing of DAN by HQ which is covered in the subsequent section.
Audit certificate & similar products	To which auditable entity does the audit certificate relate to? What are the financial years under consideration? Status (Account received/preliminary comments issued/revision of accounts received/considered for non-review/issue of non-review certificate/under QA/considered for nil comments/issue of certificate with nil comments/submission of draft comments or opinion to C&AG HQ/under C&AG HQ/issue of certificate with comments)

30.2.1.2 Configuration of key information for products (Product Key)

The product key element also may vary from product to product. It is important to note that while the products may be processed in one module, the key relating to the products may be in the same module or different module. An illustrative list is enumerated below.

- **Inspection report key**
  - What are the multiple audit observations featured in the draft inspection report?
  - What are the reference numbers for audit observations?

- What are the sub-paragraphs within each observation featured in the draft inspection report?

- **Draft PAR/TAR key**
  - What are the multiple audit observations featured in the draft DPAR/DTAR report?
  - What are the sub-paragraphs within each observation featured in the draft DPAR/DTAR report?
- **Statement of Fact key**
  - What are the multiple audit observations featured in the statement of fact?
  - What are the reference numbers for audit observations?
  - What are the sub-paragraphs within each observation featured in the statement of fact?
- **Draft paragraph key**
  - What are the SOFs linked to the DP?
  - What are the audit observations in the SOF linked to the DP?
  - What are the sub-paragraphs within each observation in the SOF linked to the DP? Note that not all audit observations of an SOF and not all sub-paragraphs in audit observations of an SOF need to make it in the DP stage)
- **Departmental appreciation note key**
  - What are the SOFs/IRs featured in the DAN?
  - What are the audit observations in the SOF/IRs featured in DAN?
  - What are the sub-paragraphs within each observation in the SOF/IRs featured in DAN?
    Note that not all audit observations of an SOF and not all sub-paragraphs in audit observations of an SOF need to make it in the DAN stage)

The product key should be used to display the links between products stored in OIOS and audit observations like a ‘hyperlink’.

30.2.2 Configuration of workflow for each audit product

The field audit offices must be able to configure separate workflows for processing of each type of audit product. This is because the actors involved in the process of preparation, finalisation and issue of audit products vary from product to product and office to office. A common workflow template for each audit product would be configured by the application administrator. The office administrators and wing administrators can use the common template or amend it to prepare their own workflow configuration for each of the audit product issued by their office. This is a one-time activity. Any subsequent change in the configured workflow needs to be possible through configuration changes by individual field audit offices.

30.2.3 Configuration of ranking parameters for each audit product, as necessary

The field audit offices and/or its functional wings in field audit offices may want to measure quality of the audit products by ranking the audit products based on parameters. This may not be necessary for all audit products. OIOS should provide the functionality for configuring the parameters based on which ranking would be decided. Most of the ranking would be allotted manually. Apart from the risk parameters, its data type, range etc., the formula to be used for calculation of the rank would also be configured in OIOS. When the individual parameter values are filled for an audit product, the rank of the audit product is auto-calculated by the OIOS system.

30.3 Actors involved

As described earlier, the workflow for processing of each of the product and thus, the actors involved would also vary from product to product and field audit office to field audit office.

Product	Actors involved
Draft inspection report	• **Audit team:** The draft inspection report is prepared and issued by the audit team (specifically the team leader issues the DIR) • **Auditable entity (External)** receives and responds to the DIR normally in the exit meeting of the audit programme.
Inspection report	• **Issuing authority:** The inspection report is issued by the issuing authority. • **Audit team:** The draft inspection report is prepared and issued by the audit team (specifically the team leader issues the DIR) • **Auditable entity (External)** receives and responds to the IRDIR normally in the exit meeting of the audit programme.
Draft PAR/TAR	• **Audit team:** The DPAR/DTAR is prepared and issued by the audit team/lead team in case of multiple teams (specifically the team leader issues the DPAR/DTAR) • **Apex Auditable entities/Government (External)** receives and responds to the DPAR/DTAR.
Statement of Fact	• **Preparer** prepares the SOF • **Reviewer** reviews and provides feedback to the SOF • **Issuing authority** is the final competent authority to approve the issue of SOF • **Government (External)** receives the SOF and gives response. • **Apex auditable entities (External)** also receives the SOF and gives response.
Draft paragraph	• **Preparer** prepares the DP • **Reviewer** reviews and provides feedback to the DP • **Issuing authority** is the final competent authority to approve the issue of DP • **Government (External)** receives the DP and gives response. • **Apex auditable entities (External)** also receive the DP and gives response.
Departmental appreciation note	• **Preparer** prepares the DAN • **Reviewer** reviews and provides feedback to the DAN • **Issuing authority** is the final competent authority to approve the issue of DAN • **Government (External)** receives the DAN and gives response. • **Apex auditable entities (External)** also receives the DAN and gives response.
Management letter	• **Preparer** prepares the ML • **Reviewer** reviews and provides feedback to the ML

	• **Issuing authority** is the final competent authority to approve the issue of ML
Audit certificate / Audit opinion	• **Auditable entity** submits the accounts and responds to preliminary comments. • **Statutory auditor** (wherever applicable) receives and responds to preliminary comments. • **Audit teams** in field audit offices audit and issue preliminary comments • Issuer issues the draft opinion/comments to the auditable entity and C&AG HQ. • **Processors** in C&AG HQ who review and approve the draft audit opinion / comments or issue queries. • **Responders** in field audit offices who respond to C&AG HQ queries.

30.4 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Defining the audit product type.
- Create a template for business data relating to the product or using existing templates.
- Configure the workflow for the product type.

Two sample illustration of workflows have been given below.

Workflow involved in audit product

- Preparation of product
- QA/QC of product within field audit offices
- Processing of products by C&AG HQ, wherever necessary.
- Issue of product
- Response to product (Response to observations featured in product)

Workflow involved in audit certificate

- Data entry of receipt of accounts.
- Communication of preliminary comments.
- Receipt of response to comments and/or revised accounts.
- Communication of draft opinion / comments to C&AG HQ for approval.
- Communication of queries from C&AG HQ to field audit offices.
- Communication of response to field audit offices.
- Approval of final audit certificate / opinion / comments by C&AG HQ
- Issue of audit certificate by field audit offices to auditable entity.

31 Drafting an audit product (07_02)

The draft audit product is the first version of the audit product. It is typically prepared by the field audit offices. The content of the draft audit product is prepared in the word processor. Apart from maintaining the business data relating to the draft audit product, OIOS would provide the following functionalities.

31.1 Generation based on a template

Some of the audit products lend themselves to be partly auto generated based on business data available within OIOS. For example, the Draft Inspection Report contains the list and description of audit observations raised during the audit programme, which can be automatically filled by the system. Also, the template might contain standard static information with interspersed dynamic field information (See illustration below).

Template:
This inspection report contains findings relating to Compliance audit of {Name of the auditable entity} covering the period from {from} to {to} was audited from {Date of audit (from)} to {Date of audit (to)} by the following members.
{List of members of audit team}

Generated portion of the report:
This inspection report contains findings relating to Compliance audit of District Educational Officer, Shimla covering the period from 2014-15 to 2017-18 was audited from 01.07.2019 to 15.07.2019 by the following members.

1. Mr. ABC, SAO
2. Ms. DEF, AAO
3. Mr. KLJ, AAO
4. Mr. RTW, Sr. Ar.

Another illustration would be that there are ten different templates or formats available for audit certificates to be issued after supplementary audit of financial accounts of Central Public Sector Enterprises. The ten different formats are listed below.

- Format/ certificate for conducting supplementary audit of financial statements and issue of comments
- Format/ certificate for conducting supplementary audit of financial statements and issue of Nil comments
- Format/ certificate for not conducting supplementary audit of financial statements
- Format/ certificate for conducting supplementary audit of financial statements, revision of financial statements and consequent issue of Nil Comments
- Format/ certificate for conducting supplementary audit of financial statements, revision of financial statements and consequent issue of Comments
- Format/ certificate for conducting supplementary audit of consolidated financial statements and issue of comments
- Format/ Certificate for conducting supplementary audit of consolidated financial statements and issue of Nil comments
- Format/ Certificate for not conducting supplementary audit of consolidated financial statements
- Format/ Certificate for conducting supplementary audit of consolidated financial statements, revision of consolidated financial statements and consequent issue of NIL comments

- Format/ Certificate for conducting supplementary audit of consolidated financial statements, revision of consolidated financial statements and subsequent issue of Comments
- Format/ Certificate for conducting supplementary audit of financial statements, revision of Statutory Auditor's Report and consequent issue of Comments
- Format of Certificate for conducting supplementary audit of financial statements, revision of Statutory Auditor's Report and consequent issue of Nil Comments
- Format/ Certificate for conducting supplementary audit of consolidated financial statements[70], revision of Statutory Auditor's Report and consequent issue of comments
- Format of Certificate for conducting supplementary audit of consolidated financial statements, revision of Statutory Auditor's Report and consequent issue of NIL comments

OIOS would provide the functionality to maintain such templates and configurations at all levels, IA&AD level, field audit offices level and its functional wing level. The publishing of templates at various levels may require review and approval by competent authority at various levels.

31.2 Linking of key documentary evidence

During and after the preparation of the draft audit product, key documentary evidence is linked to the draft audit product. The relevant phrases, portions of the draft audit product are selected and a hyperlink is added to the key document or a specific bookmarked portion of a key document. Meta-data is required for key documents.

31.3 Actors involved

The following actors are involved in drafting the audit product.

- **Template creator** will configure the template for auto generation (complete or partial) for an audit product.
- **Preparer** will create the initial draft from scratch or partially auto generated or completely auto-generated.
- **Reviewer** will review the draft audit product and provide feedback.
- **Approver** will approve the draft audit product.

31.4 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- The activities (indicative) envisaged in OIOS are listed below.
- Configuration of template for auto-generation.
- Prepare/auto-generate the draft audit product.
- Update/make changes to the draft audit product.
- Review audit product.
- Approve audit product.

[70] When a company (including a Government PSU) has subsidiaries, it prepares both individual financial statements as well as consolidated financial statements for the year. In case of Government PSUs, both statements are subject to supplementary audit by C&AG.

32 QA/QC within Field Audit Office (07_03)

The quality assurance/ QC process is a multi-level process which ensures largely the following checks. OIOS should provide for maintaining such a checklist for QA/QC. This checklist is broadly common for all field audit offices of IA&AD, but may vary slightly especially across different audit streams.

i. Is the audit observation based on well-defined audit criteria?
ii. Are the conditions described in the audit observation well supported by reasonable key documentary evidence?
iii. Are the responses of the auditable entity taken into consideration correctly?
iv. Is the audit conclusion appropriate?
v. Is the quantification of impact, where quantified, correct?
vi. Is the materiality determined by the audit team correct?
vii. Is the audit observation material enough to be featured in other products? If yes, what are they?
viii. Is the drafting of the product satisfactory?

The QA checks from (i) to (iv) assists the issuer in deciding whether to issue the audit observation or not. That is, in case of failing to satisfy the checks from (i) to (iv), the issuer might decide any one of the following.

a) Not issue the audit observation.
b) Direct collection of more records, data or information.
c) Refer the audit observation to a technical expert/another reviewer.
d) Wait for further response from the auditable entity.

The decisions c) and d) might result in issuing a supplementary product as it takes time for obtaining a technical opinion or response. However, the checks from (v) to (viii) in most cases will result in the issuer deciding to issue the audit observation with modifications to quantification, materiality, drafting. The issuer might also decide to pursue the audit observation through a specific final product. For example, the issuer might decide to pursue the audit observation through inspection report and not find it significant to pursue through an audit report. The QA/QC team would need the ability to view audit enquiries and/or audit observations which did not become part of the draft audit product. The QA/QC team may also decide to revive one or more audit enquiries and/or audit observations and include them in the draft audit report.

Business data relating to Quality assurance

- In each level of QA/QC,
    - What is the QA/QC level?
        - For audit observations in Compliance audit assignments
            - DIR -> IR, IR -> SOF, DIR -> SOF, SOF -> DP, DP -> AR
        - For audit observations in Performance / Theme based audit assignments
            - DPAR/DTAR -> SOF, DPAR/DTAR -> DP, SOF -> DP, DP -> AR
        - For audit comments / opinions in financial audit assignments
            - Draft NRC -> NRC, Draft NC -> NC, Draft opinion -> opinion, Draft comment -> Comment, Draft SC -> SC
    - Who did the QA/QC? (Generally multiple levels)
    - When was it done?
    - For each observation (and each sub-paragraph)
        - What is the result of each of the QA checks?

- What does the QA person propose? (Not issue the observation / Defer the observation for collection of further data, technical opinion, reply from auditable entity / issue the observation with modifications in draft, quantification, materiality.
- In case of request for further details,
  - When was the request made?
  - Who made it?
  - To whom it was made to?
  - Reason (Additional key document, information, technical opinion)
  - Details of request
  - Due date of response
  - Whether response was received (yes/no)
  - If yes,
    - What was the response?
    - Who responded?
    - Details of response
    - Attachments with response
  - What is the final decision of QA team after the due date?
- Is the observation material enough to be featured in an audit product? (More relevant in case of QA of DIR, where the QA team can specify whether the audit observation is material enough to be featured in audit report).

32.1 Actors involved

The actors involved are the following.

- **QA team:** The team members perform the quality assurance checks, document their view, make changes, request for further data, records and information from audit team, requests for an opinion from external expert.
- **Audit team:** Receives request for additional data, record or information and responds to the same.
- **External expert/Additional reviewer:** Receives request for technical opinion and responds to the same.

32.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Configuration of checks to be performed by the QA/QC.
- Inspect the audit observations against the evaluation criteria and record result of QA/QC.
- Communicate with audit team for additional information.
- Receive additional information from audit team.
- Request and receive technical expert's opinion.

33 Finalisation and issue (07_04)

After the preparation of the draft audit product, the final audit product may be finalised by the field audit offices themselves or submitted to C&AG for processing and finalisation. The finalisation involves deriving assurance on the quality and appropriateness of audit product on behalf of HOD and C&AG respectively.

33.1 Finalisation of audit products within field audit offices

During the finalisation, the “processor” team in the field audit office can do one or more of the following.

a. Verify the Key documentary evidence completely or on a selective basis.
b. Raise questions or queries for clarification.
c. Direct to gather additional information, data and/or records.
d. Conduct supplementary field audits.

During the processing (multiple iterations), the “processor” team of field audit office in a consultative manner with the functional wings of C&AG HQ may also decide to defer or drop an audit observation, if found necessary.

33.2 Finalisation of audit products by C&AG HQ

During the finalisation, the field audit office may send the entire audit product as a whole or just parts of it (For example, draft performance audit reports) referred to as ‘material’ to be included in the audit product. The processing of the draft audit product happens in several iterations which are referred to as ‘journeys’. The key documents relating to material are marked by the field audit offices using ‘hyperlink’ feature of word processor, wherever necessary. In each journey, the processors in C&AG HQ can do one or more of the following.

a. Verify the Key documentary evidence completely or on a selective basis.
b. Review the clarifications received on queries which were raised earlier.
c. Raise further questions or queries for clarification.
d. Direct to gather additional information, data and/or records.
e. Conduct supplementary field audits/work.

There will also be iterations (“pre-bond copy” or “bond copy”) where the draft of the entire C&AG Audit Report would be prepared and submitted. As a final round, a presentation of summary of findings of the draft Audit report is made to the C&AG for this review.

During the processing, the processors of C&AG HQ in a consultative manner may also decide to defer or drop an audit observation, if found necessary. The questions/directions by the processors in C&AG HQ is referred to as ‘queries’ and the response provided by field audit offices is referred as the ‘annotated’ version. While processors range from a hierarchy of desk officer to C&AG of India, the responders range from a hierarchy of field audit teams to head of the Field Audit Office.

This process is envisaged to be performed by a combination of ‘Track changes’ and ‘Review with comments’ features of a word processor in the OIOS ecosystem. The OIOS ecosystem in itself will not capture individual query-wise data or information in a database table structure. It would be available as part of an attached word document. However, the process of communication between field audit offices and C&AG HQ would be part of OIOS. Thus, OIOS would keep track of the journeys between C&AG HQ and field audit offices.

Business data relating to processing of material to be featured in audit product

- Name of the material
- Description of the material
- Name of the audit product
- Reference to one or more specific assignments/sub-assignments in the annual audit plan?
- If yes, what are the assignments?

- Status of the material (Under-processing/Completed/Pre-bond/Bond copy/Suo-motu corrections/Final product)
- Processing communication history
  - Date of submission to processor
  - Remarks during submission
  - Attachments relating to the material submission including actual content and annexures
  - Date of communication from processor
  - Remarks during communication
  - Attachments relating to the communication including actual content and annexures
  - Status change

33.3 Post finalisation activities

The activities after finalisation such as translation into the local language / Hindi, printing, submission to the President/Governor and tabling of the reports happen outside the OIOS ecosystem. However, certain business data elements alone would be captured in OIOS.

Business data relating to post finalisation activities of audit report

For each of the relevant field audit offices,

- Name of the product
- Final audit product in English language
- Final audit product in other languages
- Date of submission to President/Governor, if applicable
- Date of laying in the legislature, if applicable

33.4 Ranking of audit products

After the finalisation and issue of audit products, a field audit office and/or its functional wings would fill the values for the rank parameters which were configured earlier. This ranking is not mandatory for all types of audit products. The OIOS system auto-calculates the rank of the product based on the formula that was configured earlier.

33.5 Actors involved

The following are the actors involved.

- **Processors** in review material submitted for finalisation.
- **Responders** in field audit office act as the point of communication to the queries of the processors.

33.6 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Creation of queries through word processor (using “inline” or “Comment” features and response thereto either or in “annotated format”).
- Response to queries through word processor.
- Closure of queries through word processor.
- Communication of queries from processors to responders.

- Response of field audit offices to processors.

34 Receive response[71] (07_05)

Once, a response is received through the 10: Communication module, the relevant employees are notified of the response. The employees responsible for processing of the reply peruse the reply to decide on the further course of action. The same may be intimated to the relevant auditable entities via a "rejoinder".

Indicative business data that are common across all audit products and all field audit offices

a) **Response of auditable entity:** Any response received form the auditable entity relating to the product is also captured by OIOS. The response might be received through the digital communication interface or through traditional channel. In case of receipt through traditional channel, the response is uploaded manually into OIOS.

- What was the response[72] of the auditable entity for each audit observation (and sub-paragraph) in the audit product? In case of receipt of response from the auditable entity,
- Who responded?
- Date of reply
- Nature of reply (interim / final)
- Whether the reply relates only a few of sub-paragraphs listed in the observation?
- If yes, for each sub-paragraph in the reply
  - Whether the auditable entity accepted the audit observation (accepted / partially accepted / not accepted)?
  - Detail of reply
  - Attachment relating to the reply
  - Does audit agree with the reply of auditable entity (reply is acceptable / reply is not acceptable / reply requires reconsideration)?
  - What is the decision of audit (Not pursue observation further / reiterate or update an audit observation)?
  - Remarks relating to decision
  - Who made the decision?
  - Date of decision
- If no, for the audit observation as a whole,
  - Whether the auditable entity accepted the audit observation (accepted / partially accepted / not accepted)?
  - Detail of reply
  - Attachment relating to the reply
  - Does audit agree with the reply of auditable entity (reply is acceptable / reply is not acceptable / reply requires reconsideration)?

[71] This module covers responses to audit observations and draft audit products (e.g. draft IRs, draft material in C&AG's Audit Reports). Responses to issued IRs and tabled C&AG's Audit Reports are covered under follow-up and not in this module.

[72] The response from the auditable entity is general, cross-cutting across various audit observations. The response once received need to be mapped to appropriate entities. The response may also contain replies to draft recommendations.

- What is the decision of audit (Not pursue observation further / reiterate or update an audit observation / required action has been taken by the Department)? Remarks relating to decision
- Who made the decision?
- Date of decision

34.1 Actors involved

The following actors are involved in the receipt and processing of response to audit products.

- **Auditable entities (external)** send responses to audit products.
- **Processors** of replies receive, process and make decisions on the rejoinder.

34.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Receive response for an audit product.
- Process the response for the audit product.
- Communication a rejoinder to the auditable entities, wherever necessary.

35 Recommendations (07_06)

During the preparation of audit conclusions in the audit products, the field audit offices may come up with one or more recommendations[73] for the auditable entities to consider. The auditable entities may choose to accept or not accept the recommendations. Hence, OIOS should provide the functionality to add recommendations to an audit product. The indicative business data relating to audit recommendations is listed below.

Indicate business data relating to audit recommendations

- Audit product reference number
- Audit recommendation reference number
- Description of the recommendations
- List of auditable entities that are related to the audit recommendations.
- Stage (Draft/Final)
- Status of acceptance by the auditable entity (Yet to be communicated/Fully accepted/Partially accepted/Not accepted)

35.1 Actors involved

The following are the actors involved.

- **Recommendation trackers** who add the data relating to recommendations, acceptance of recommendation and implementation status of recommendations.

35.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Add recommendations.

[73] The recommendations in the draft audit product are called as 'draft recommendations'. The response of the auditable entity is also captured.

- Track acceptance status of recommendations.
- Trace implementation of recommendations.

36 T&M phase of Audit reporting module

36.1 API Integration with auditable entities (07_07)

The most efficient way to handle this API interface is as an interface, where feasible, between IFMS (Integrated Financial Management Systems) of the State/UT Government and PFMS (Union Government). OIOS project envisages establishing these interfaces in the future phases. The implementation of these interfaces will be staggered and are based on readiness of the IFMS and PFMS systems. Hence, this sub-module is proposed to be implemented as part of future phases.

08 Audit Follow-up

This module will aid in following up on action taken by the auditable entities on the audit products/ observations that were communicated to the auditable entity. While the field audit offices produce several audit products (interim and final), formal follow-up processes exist in two cases:

- The first are audit observations featured in a product called 'Inspection Reports'[74] which are followed-up through an internal mechanism within IA&AD.
- The second are audit observations featured in the audit product called C&AG's audit reports, which are followed-up through two special committees constituted in the state and central legislatures. The committees are the Public Accounts Committee (PAC) and the Committee on Public Undertakings (CoPU)[75].

In some cases, e.g. supplementary comments of C&AG on the financial statements

It is pertinent to note that some of the audit observations featured in the Inspection Report might have been included in the audit report (through a mechanism of issuing SoF and DP that is discussed in detail in **'07 Audit reporting'**). The status of these observations along with the sub-paragraphs, i.e., / part observations as 'Fully included in audit report' or 'partially included in the Audit report'. The follow-up mechanism for these observations that were fully included and sub-paragraph, i.e., part observations in case of partial inclusion will be through PAC/COPU[76].

The exact processes and activities involved in the follow-up of audit report through PAC and COPU varies from state to state and between state and union as well. This is one unique case, where the terminologies and processes used in different states cannot be made uniform as external entities are involved. Hence, this would be a module which would require considerable amount of configurability. The process is further explained in the sub-module (08_02).

37 IR/DAN Follow-up (08_01)

The first step in this process is to receive the reply from auditable entity.

37.1 Receipt of reply from the auditable entity and allocation/mapping

Most of the replies[77] from the auditable entity are received through traditional paper-based mail or fax (referred to as **'DAK'**). Some of them are received through email. A few of the field audit offices have either a common web-based IT application or interface between the Audit Office's IT application and the State Government/ Auditable Entity's IT applications. In such cases, the replies from auditable entity and responses to the replies from the field audit offices are communicated through these applications/interfaces. In the case of such IT enabled communication, OIOS would have to use an API mechanism to push/pull information regarding replies and responses.

[74] Where observations featured in Departmental Appreciation Notes (DANs) and Management Letters (MLs) are to be followed up independently, the same mechanism can be used.

[75] In some States, there is a separate Legislative Committee for following up observations featured in the C&AG's Audit Reports on Local Bodies.

[76] The follow-up for audit observations which is featured in the C&AG's audit reports will not be through any other audit product (For example, Statement of Fact), even though the audit observations are part of the product.

[77] The replies may be received in multiple languages.

The actors responsible for following up on replies are allotted very specific roles. The exact workflow of allocation of the receipt should be configurable as it varies from between field audit offices. During the allocation of receipt, meta-data is captured by the actors in the workflow.

Illustration of a workflow for allocation of receipt
In the case where 'DAK' is received, the 'DAK Scanners' will scan the relevant letter/mail and upload it as a new 'receipt' and allocate it to the relevant pursuers. In order to auto-allocate a 'DAK' to the relevant section, OIOS needs to provide a functionality to set up business rules for allocation which would vary from one field audit office to another.

In case of receipt of reply through email, the wing administrator pulls the email into the OIOS system and allocates it to relevant section. The relevant pursuers in the section will process the reply and issue a rejoinder (response) after seeking approval from competent authority. The rejoinder is communicated either through the digital communication interface or through traditional channels (paper-based, or e-mail, if e-mail addresses are available). For further details regarding various modes of external communication, '**10: Communication module'** may be referred.

When an observation of inspection report is being considered in draft audit products, then the OIOS system must alert the user of such inclusion. In case where an observation of inspection report is featured in a finalised audit product, then the pursuance of the same through Inspection reports should not be allowed.

Further, the follow up of outstanding audit observations in previously issued inspection reports is one of the activities carried out by the audit team during their field visits. Hence, at the time of field audit/audit execution, OIOS should provide a facility to view the outstanding observations, upload replies received from auditable entities, process the reply and recommend rejoinders. The recommendations for rejoinder would be considered by the competent authority or QA/QC team for perusal and approval.

37.2 Mapping of replies

Once the replies are received from the auditable entity, it needs to be mapped appropriately. It is important to understand that one reply might contain responses to one or more audit observations and / or sub-paragraphs. OIOS should assist in mapping of replies to the following.

- One or more audit observations under each related audit product.
- One or more sub-paragraphs under each related audit observation and under each related audit product.

The indicative business data relating to IR follow-up is listed below.

Indicative business data relating to IR-follow up

- Date of receipt of reply
- Reply reference number
- Reply date
- Mode of reply (Paper, fax, email, digital interface)
- Who sent the reply?
- Nature of reply (interim / final)
- Whether the reply relates only a few of sub-paragraphs listed in the observation?
- If yes, for each sub-paragraph in the reply,

- Whether the auditable entity accepted the audit observation (accepted / partially accepted / not accepted)?
    - Detail of reply
    - Attachment relating to the reply
    - Does the pursuer agree with the reply of auditable entity (reply is acceptable / reply is not acceptable / reply requires reconsideration)?
    - What is the decision of pursuer (Not pursue observation further / reiterate or update an audit observation / Transfer without recourse / Transfer subject to finality being watched by auditable entity/ required action has been taken by the Department)?
    - Remarks relating to decision (As part of workflow)
    - Who made the decision? (As part of workflow)
    - Date of decision (As part of workflow)
- If no, for the audit observation as a whole,
    - Whether the auditable entity accepted the audit observation (accepted / partially accepted / not accepted)?
    - Detail of reply
    - Attachment relating to the reply
    - Does the pursuer agree with the reply of auditable entity (reply is acceptable / reply is not acceptable / reply requires reconsideration)?
    - What is the decision of pursuer (Not pursue observation further / reiterate or update an audit observation / Transfer without recourse / Transfer subject to finality being watched by auditable entity / required action has been taken by the Department)? Remarks relating to decision
    - Remarks relating to decision
    - Who made the decision?
    - Date of decision
- Details relating to communication of rejoinder
    - Rejoinder reference number
    - Rejoinder date
    - Mode of rejoinder (Paper, fax, email, digital interface)
    - Who sent the rejoinder?
    - To whom (including endorsement)?

37.3 Formal follow-up mechanisms

There are three formal follow-up mechanisms that serve as a space for exchanging communication between IA&AD and the auditable entity. These meetings typically cover groups of auditable entities.

a) Apex committee meetings
b) Audit committee meetings
c) Joint sittings.

Apart from the discussions relating to specific issues, the meetings may also involve handing over of responses of auditable entities in person. The responses received during the meeting then trigger the 'Receipt' mechanism in '**10: Communication module**'. The indicative meta-data to be maintained relating to these mechanisms is listed below.

Indicative business data relating to formal follow-up mechanisms

- Date of meeting

- Type of meeting (Audit committee meeting, Joint sitting, Apex Committee meeting)
- Related auditable entity
- Attachments
- Minutes of the meeting
- Responses received during the meeting

37.4 Actors involved

The following are the actors involved (based on illustrated workflow).

- **DAK Scanners** scan the paper-based response and allocates to relevant pursuers
- **Wing administrators** pull the response through email and allocates to relevant pursuers.
- **Pursuers** reviews the reply from auditable entity and propose necessary action including settlement, dropping or not pursuing the audit observation or specific sub-paragraphs of observations.
- **Reviewers** review the proposal and provide feedback.
- **Approving authority** is the competent authority for approving proposals for settlement, dropping and not pursuing further.

37.5 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below. These set of activities may be repeated iteratively.

- Receipt of reply
- Processing of reply and initiate proposal of rejoinder, if necessary
- Review of proposals of rejoinder
- Approval of rejoinder proposals
- Communication of rejoinder to auditable entity

38 PAC/COPU/Other Legislative Committee Follow-up (08_02)

As explained earlier, the audit observations that were featured in the C&AG's Audit Report are followed-up through two committees, viz., PAC and COPU[78]. The workings of both the committees, including processes and activities are similar. COPU is responsible for following up C&AG's Audit Reports on public sector undertakings while PAC is responsible for taking up Audit Reports relating to civil departments of the Union and the State Governments. Each committee has its own secretariat which assists the members of the committee in discharging their duties duly assisted by IA&AD officials.

After the C&AG's audit report is tabled in Parliament or the State Legislature and stands referred to PAC or COPU, the Department / Government submits an Explanatory Note (EN)[79] on all the paragraphs/ observations featured in the audit report. The explanatory note is submitted in English and/or the official language of the committee. The Explanatory Notes are vetted by the respective Field audit offices with remarks and sent to the secretariat of the PAC committee for necessary action; often, this vetting takes place through an iterative process. The vetting remarks (iterative cycle)

[78] Apart from Central PAC and COPU for the Union Parliament, there is a PAC and COPU for each State Legislature and UT with Legislature.

[79] Different terminologies are used by different State Governments – e.g. Detailed Explanation (DE)

offered by the related field audit offices to the PAC committee may be referred to as 'PAC brief' or equivalent term. If there is no remark to offer, then it is marked as 'No further remarks'. OIOS should facilitate to monitor whether the EN was received within the stipulated time frame.

In addition to the written explanations on all observations featured in the C&AG's Audit Report, the PAC/ COPU take up selected Audit Reports or observations for "oral examination". The process followed is as follows:

- The respective Field Audit Office often (not always) assists the PAC/ COPU Secretariat in selection of Audit Reports/ observations for oral examination. The State Government officials associated with the selected audit observation[80] are then asked to give evidence before the PAC/ COPU in a Committee Meeting.
- For each audit observation/ Audit Report selected for oral examination, the respective Field Audit Office often (not always) prepares a draft 'Memorandum of Important Points' (MIP) and sends it to the PAC/ COPU Secretariat for assisting the PAC/ COPU in the oral examination.
- After the submission of evidence by the Department/Government during the Committee meeting, the PAC provides suitable recommendation for either the audit report paragraph to be settled or for taking further action. The PAC then publishes a report containing the recommendations arising out of the oral evidence and discussion.
- The Department/ Government prepares 'Action Taken Report (ATR)[81]' on the PAC Recommendations, which are got vetted by the respective Field Audit Offices.
- The PAC recommendations, as reflected in their Reports, are taken up for discussion in subsequent meetings, after considering the ATNs/ ATRs and vetting remarks thereon.

Note: The first reply of the Department / Government to the audit observations in audit reports are called as 'Explanatory notes[82]'. The subsequent replies on PAC recommendations are taken as 'Action Taken Reports'. The terminologies across the legislative committees of States, UT (with legislature), and Central Governments vary and OIOS should provide flexibility of these varying terminologies. Since, the terminologies are used by both IA&AD and external agencies, it is difficult to build a uniform terminology in this case.

In the case of Central PAC, the ENs/ATRs/vetting remarks are uploaded on the CGA's Audit Para Monitoring System (APMS) by Department / Government. However, such an IT enabled mechanism is mostly absent in the States.

The OIOS ecosystem should integrate with the Audit Para Monitoring System and provide a similar platform for each of the field audit offices for states and UTs with legislature. Though, the actual process of the meetings and deliberations may be outside the system, OIOS should provide a platform for post facto data entry and communication to the secretariat of the committees.

Indicative business data for audit follow-up in PAC/COPU
For each Audit report

- Audit Report Number

[80] Typically, of the rank of Secretary/ Principal Secretary/ Additional Chief Secretary in the State Government

[81] Sometimes, the term Action Taken Note (ATN) is used in this context. However, in some States, ATN is the equivalent of the Explanatory Note.

[82] A view to list audit paragraphs in a report / for reports where first explanatory note had not been received as on a particular date/within due date. The ability to view whether explanatory note has been received on a particular report or paragraph should be provided.

- Audit Report Type (SFR, Revenue Sector, PSUs, etc.)
- State
- Report Year
- Paragraph reference Number(s)
- Sub-Paragraph Reference Number(s)
- Title (with hyperlink to bookmarked section of the digital document of audit report)
- Detail
- Amount
- Status
- Mapping between audit paragraph and explanatory note
  - Explanatory Note Number
  - Detail**
  - Status (Pass over / Memorandum of Important points)
  - PAC/COPU brief**

For each explanatory note,

- Explanatory Note Number
- Received on
- Reference Letter Number
- Attachment

For each PAC/COPU meeting

- Meeting reference number
- Date of meeting
- List of attendees from field audit offices
- List of audit reports discussed
- Selected topics or paragraphs for oral discussion

For each PAC/COPU report**

- Committee Number
- Year
- Assembly Number
- PAC Report Number
- Meeting reference number
- Description
- Related Audit Report No
- For each recommendation
  - Recommendation detail
  - Serial Number (Reference number for recommendation)
  - Audit Report Para Reference Number
  - Further reply
  - Recommendation of the committee (Settled / Further detail or action is required)

** represents bilingual information (both English and official language of the committee)

38.1 Actors involved

Section of field audit office facilitating follow-up by PAC/COPU is responsible for vetting of EN, ATN/ATR, marking of MIP and preparation of brief to PAC.

Auditable entities (external) is responsible for submission of EN, ATN/ATR and evidence during hearing meetings.

PAC/COPU including its secretariat (external) reviews EN, ATN/ATR in the light of PAC/COPU brief and makes recommendations.

38.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Data entry of the Audit Report which got placed in Parliament/ Legislature
- Receipt of Explanatory notes and entry into OIOS.
- Vetting of EN and preparation of PAC brief
- Communication of PAC brief
- Vetting of ATR and preparation of PAC brief
- Data entry of PAC report which was released by PAC (including PAC Reports on follow-up of recommendations in earlier PAC Reports)

39 Recommendations (08_04)

The field audit offices would follow-up on the accepted recommendations which were made by them during an audit assignment. The field audit offices would verify whether the recommendations were fully or partially implemented or not implemented at all. This may be taken as a separate follow-up audit assignment or as part of other audit assignments (compliance audit / performance audit). They may also be verified periodically. Hence, OIOS should provide the functionality to track the implementation status of recommendations.

Indicate business data relating to follow-up of audit recommendations

- For maintaining implementation status of a recommendation,
    - When was the implementation verified?
    - Assignment through which implementation was verified?
    - Status (Not implemented/Partially implemented/Fully implemented)
    - Remarks regarding implementation
    - Attachments relating to implementation

39.1 Actors involved

The following are the actors involved.

- **Recommendation trackers/Audit team leaders/Audit managers** maintain implementation status of recommendations.

39.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Trace implementation of recommendations.

40 T&M phase of Audit follow-up module

The following is envisaged for the time and material phase of the project.

40.1 API Integration (08_03)

The OIOS system envisages API based interface for the communication between the field audit offices, the committees and the auditable entities. Presently, a system ‘Audit Para Monitoring System (APMS)’ is used for monitoring the paragraphs featured in the audit reports relating to Union Government.

These are followed up by the PAC and COPU committees of Parliament. OIOS, through an API interface, must be able to push and pull relevant information to/from APMS. A similar set of API interfaces need to be envisaged for all state committees and UT (with legislature) committees.

09 Data Collection platform

This module aims at providing a platform for IA&AD to manage its data collection activities. There are various processes during which data collection becomes very essential. The data collection requirements are both periodical and adhoc. The allocation of access to data collection may range from specific audit assignment to functional wings of FAO to field audit offices. The following are some of the use cases for data collection.

- C&AG HQ desires to collect data from all or selected field audit offices on an ad-hoc basis (either directly or through functional wings of FAO).
- The field audit office desire to collect data from its branch offices.
- The field audit office desires to collect data from its functional wings including its branches/sections.
- One nodal field audit office desires to collect data from its peers (in case of All-India Performance audit, statistical information for audit reports, etc.)
- One functional wing of FAO desires to collect information relating to auditable entities by the audit teams during the audit execution as part of audit assignment.
- **Surveys**: A field audit office desires to collect information from citizens or specific sub-set of citizens (beneficiary survey) as part of audit assignment. Normally this is done by an audit team onsite and filling up of the form by the audit team[83] and/or the citizen.
- **Audit toolkits and checklists**: The same platform will be used to collection information for an audit toolkit (For more details on Audit tool kits, please refer '**05-Audit Design**').

Thus, OIOS would provide a platform with the following functionalities regarding data collection.

i. The first step in data collection is designing the format in which data can be collected. It is essential to understand that once created, the data collection format ay undergo a change until it is finalised explicitly. When there is a change in the design, the decision on whether to go back to the earlier samples or programmes and rework or not would be based on feasibility. However, the data collection that gets conducted after the change would be in-compliance with the change.

ii. Then, the system would provide ability to allocate access to collect information. In case of internal stakeholders only, the access may need to be provided to user or user groups or field audit offices or specific audit assignments. In the case, where the data collection activity requires involvement of external stakeholders.

iii. Thus, there may be a need to publish both in public domain (through C&AG website as an add-on) and internally within the OIOS system (detailed in subsequent sections).

iv. The process of collection of data involves filling up of the data collection by the citizens (beneficiaries) or internal users of OIOS system. The designer/administrator of the data collection assignment would need to monitor the progress of collection on a real-time basis.

[83] The audit team may obtain a signature etc. of the citizen, whose responses are being gathered.

v. After the completion of the collection, the designer/administrator would need to download the data, consolidate the data and perform data analysis on the same[84].

vi. Further, once a data collection assignment is undertaken, the design of data collection and/or data must be available for use by IA&AD through central repository of data collection design templates or restricted access[85].

41 Design data collection kit (09_01)

A designer must be able to create a tool kit from scratch. A designer must also be able to search through the central library and reuse a data collection kit which is stored in the Central repository. A data collection kit typically contains questions and/or data fields which would be referred to as 'elements'. The elements in the data collection kit is mostly filled manually by the data collectors. However, there may be some elements which can be answered based on external data. Thus, the different types of elements that a collection kit may include are listed below.

- Data fields with various data types (such as integers, decimal, range, text, date, time)
- Multiple choice questions where one or more choices can be selected as answer.
- Multiple Choice questions and 'Other' option.
- Ranking of choices
- Capturing geo-point or geo-trace.
- Capturing date/timestamp of collection.
- Uploading audio, image, video or other files.
- Auto-calculated data fields based on answers of other questions (based on internal or external data).
- Dynamic selects based on master data validation.
    - Master data resides inside OIOS (For example, user id of OIOS)
    - Master data from external data (csv or Excel)
- Cascading selects. For example, selecting a city by selecting a country, then a state (based on selected country), then a city (based on the selected state).
- Supporting documentation (files in various formats, or references/ links to other files)

The collection kit would also provide ability to skip elements based on a logic. For example,

1. Are there children below two years in the family?
2. If Yes, then
    - Name of the child:
    - Gender: M/F
    - Date of birth: (DD/MM/YYYY)

The elements could be arranged in groups. There can be a group of elements nested within a group. There can also be repeat-group elements, where the number of groups is not known before hand and varies on a case to case basis. For example, capturing name, gender and age of all family members of a BPL family. It may be mandatory to answer one or more elements. The elements may be in multiple

[84] Maintaining the confidentiality of the individual data collected through beneficiary surveys is important. While aggregated data is often included in Audit Products, individual responses may reflect criticism of the performance of specific Government/ PRI officials and needs to be handled in a sensitive manner.

[85] The central repository will usually NOT contain the contents of the data collected, only the structure and the detailed questions.

languages. For example, the beneficiary surveys are typically prepared bi-lingually with English and the local language (say Hindi or Gujarati or Bengali); the administration of the beneficiary survey is usually in the local language.

The designer may also want to collect data in a tabular or grid format (with or without knowing max number of rows beforehand). The designer will however be able to specify the data columns and their types (integers, decimal, text, date, time, look-up fields with internal and external data validation). After the design of the data collection kit, it is reviewed and approved by competent authority. The design of the data collection kit is subject to variation until it reaches 'finalised' status. Hence, any change in the design must be notified to relevant stakeholders.

Further, the data collection tool kit and data[86] may be published to the central repository after necessary checks by the Publisher. It is also required to store other meta-data about the data collection kit. The indicative business data to be stored for the data collection kit.

Indicative business data for meta data for data collection kit

- Reference Number
- Name of the data collection kit
- Description of the data collection kit
- Collection type (Beneficiary survey, audit tool kit, consolidation)
- Date of closure of collection in case of public data collection
- Created by
- Created on
- Status (created, in pilot, finalised)
- Key words
- Classification
- Is published[87] in central repository?
- If yes, Published by and Published on
- History of updates
- Link to assignments which used this data collection
- Link of field audit offices which used this data collection

41.1 Actors involved

The following are actors involved in the tool kit design. OIOS will only capture the finally approved toolkit and not the iterative process of development and finalization.

- **Designer** proposes a design for data collection kit.
- **Reviewers** reviews the data collection kit and provides feedback.
- **Approver** approves the data collection kit.
- **Publisher** publishes the data collection kit after checks.

42 Allocate access (09_02)

This sub-module provides a platform to allocate access by directly allocating to public or users or user groups or field audit offices or specific audit assignments. In the case of internal stakeholders, they must be able to send feedback regarding the data collection kit which may lead to redesign of the kit.

[86] The data contents, if published, will have restricted access.

[87] After seeking approval from competent authority.

In case of redesign, the previously collected data must be intact and re-collection/edit must be allowed.

42.1 Public

Collection of data from the public is relatively rare. The only common case for such data collection is for beneficiary surveys as part of Performance audits or subject matter-based compliance audits.

In the case of the public, there are many ways in which data collection could be performed. The first method could be by printing the survey form and getting it filled by the public and the collected data is then manually re-entered by those who are responsible for the same. The second method could be by accessing the form through the application and the survey is filled in by the audit team on behalf of the public and the responses are then authenticated by the public through physical signature/ thumb imprint[88]. The third method is by downloading a digital form (pdf or word) version of the collection kit and emailing it to a distribution list[89]. After receiving reply in the form of filled form, the pdf or word document is uploaded. During the upload, the solution should automatically be added into the system (without the OIOS user having to manually update the collected data).

In rare cases, the data collection kit could be published on the C&AG web-site for the public to fill the collection kit (survey) with a choice to fill in any of the languages that are available. The data collection gets closed on the specific date and the collected data is analysed.

42.2 Users

In the case where data collection is meant for specific users in IA&AD, this option is chosen. Once the specific user(s) is added, a notification is sent to the user. The user then views the data collection kit and fills the kit and submits the information. Upon change

42.3 User groups

User groups are (similar to distribution lists created in email) groups of users created in this module. Once attached to a collection kit, a notification is sent to all users of the group. The users of the group then view the data collection kit and fills the kit and submits the information.

42.4 Field audit offices

In the case where data is to be collected from field audit offices[90], the office administrators (or other designated roles/ posts[91]) of the field audit offices are given access to the same. The office administrator may in turn delegate the data collection kit to relevant users such as wing administrators or others. The office/wing administrators also have to certify that the data upload has been approved by competent authority. Upon completion of collection of data from within an office, the same is submitted to the administrator of the data collection activity. The data collection exercise is considered complete, when the data is received from all relevant field audit offices.

[88] Similar to mechanism of authentication of documents described in **'06: Audit Execution'**. Often, the authentication is done by the representative of the auditable entity.

[89] This would be an approach that could be considered in situations such as, for example, obtaining responses from recipients of Post Matric scholarships.

[90] The request for data might come directly from C&AG HQ or through the respective functional wings of C&AG HQ.

[91] E.g. Secretary to the HoD, or the PS to the DAG (Administration)

42.5 Audit assignments

In many cases, where the data collection kit is to serve the purpose of being an audit tool kit, they are attached to elements (objective/sub-objective/audit question) of Audit design matrix. The same element also contains the information regarding the relevant auditable entities. Hence, when an audit team is given a programme for an auditable entity, all relevant data collection kits need to be visible to the team members. The members of the audit team fill the data collection kit and submits the same after completion of the field audit / audit execution. If there is a change in the design, all the team members who are currently undertaking the audits are issued a notification. However, there may be requirement for re-collection of data with regard to changed design in the completed audits. This decision to re-collect data in such cases will be made on a case-to-case basis. In case of re-collection, the previously collected data is to remain intact.

42.6 Actors involved

The following are actors involved in giving the access.

- **DCK Administrator** assigns access to the data collectors.
- **Data collectors (internal)** receive notification, delegate and/or collect data and submit data.
- **Public (External)** fill in the data collection kit and submits data**.**

43 Monitor data collection (09_03)

This sub-module provides a platform for DCK Administrator and Audit manager to monitor the progress of data collection. They also monitor feedback received from the data collector and propose changes to be made in the design of collection kit, if necessary. Apart from the number of submissions/re-submissions, other meta-data such as location, date and time of submission/re-submission are also visible to the DCK Administrator/Audit manager. They can also view/download the data collected at any point of time.

43.1 Actors involved

The following are actors involved in monitoring.

- **DCK Administrator** and Audit manager monitors collection of data and upon completion of collection activity, they can download the data

44 Consolidate and analyse data (09_04)

This sub-module provides a platform to view consolidated data upon completion of data collection and perform basic analysis. Upon submission of data by all collectors, or when the DCK Administrator renders the collection exercise complete, the system would provide a facility to consolidate the data elements (and its sub-elements) and download the data in CSV or Excel or JSON. In case of CSV, multiple files would be necessary in case of sub-elements and the same will be reflected as multiple sheets (appropriately named). In case of JSON, the concept of sub-elements would be taken care by the schema.

The data may be published in the form of MIS reports / dash board after building the same using the '**13: Business Intelligence module**'. The indicative business data for meta-data of a data set is listed below.

Indicative business data for meta-data of data set
• Reference number

- Name of the data set
- Description of the data set
- List of relevant auditable entities
- Keywords
- Period to which data belongs to
- Date of Completion of collection
- Link to download data (CSV, Excel, JSON)
- Link to data collection kit template

44.1 Actors involved

The following are the actors involved in the process of consolidation and analysis of data.

- **DCK Administrator** renders the collection exercise complete, consolidates and analysis data. The collection kit may be published in the Central repository, after seeking approval from competent authority.

44.2 Activities envisaged in OIOS (for the module as a whole)

The activities (indicative) envisaged in OIOS are listed below.

- Preparation of a data collection kit.
- Review of a data collection kit.
- Approval of data collection kit by the competent authority.
- Publish an audit tool kit for use.
- Provide access to data collectors.
- Update a data collection kit and re-publish after seeking approval from competent authority.
- Search for relevant data collection kit stored in central library.
- Reuse a data collection kit with or without changes.

10 Communication

This module facilitates both internal communication (within IA&AD) and external communication (outside IA&AD, For example, auditable entities). This module is traditionally referred to in IA&AD as 'DAK[92] management system'. The communication is received either through API based digital interface, uploads through a web link, e-mail, fax, regular mail (post). They are then transferred to the relevant dealing hands through a workflow[93] process. After processing the communication received, it is either filed for information or acted upon. The action taken is dispatched through API based digital interface, e-mail, fax, regular mail (post). The module can also consider interfacing with NIC's e-office receipts module.

45 Receipts (10_01)

This sub-module provides a platform to receive communication from outside OIOS system (from outside and within IA&AD) in the following formats. Multiple languages need to be supported.

- Regular mail (paper-based communication);
- Fax;
- E-mail;
- Upload through web-link;
- API[94] based interface (to systems like OCAMP, APMS etc.,);

The sub-module also provides the functionality to allocate responsibility (through a configurable mechanism) for processing the communication.

In case of regular mail, fax, e-mail, and communication received through API, where OIOS generated reference number is not available, the OIOS system would not be able to trace the responsibility trail. The first point of receipt would be the field audit office mail supervisor. The inward communication ('Receipt') is generally categorised[95] as 'Communication from C&AG office', 'Letter by name to HOD', 'Letter by name to GO[96]' and 'Other mail'. The office mail supervisors record the receipt of the communication by filling specific set of meta-data that is managed by them. They then transfer the receipt to the next level. The typical levels in the transfer chain of receipt are Wing mail supervisor (optional) -> Branch -> Section -> dealing hand (optional). At every stage, it may be sent to more than one receipt, for example one or more wing mail supervisors. After receiving the receipt, the dealing hand or the section attaches the receipt as an attachment / entity in the OIOS system. For example, reply to an inspection report, Statement of Fact, etc.

In case of upload through web link or API interface where the reference number generated by OIOS is available, the OIOS system would be able to automatically identify the dealing hand / section and allocate the receipt. Meanwhile, the wing mail supervisor (optional), relevant branch and section would receive an alert about the receipt, through which they can view the receipt if necessary. Then,

[92] Also referred to as 'Purport'.

[93] The workflow may be manual or electronic. In case of manual workflow, there is a need for electronic monitoring of the disposal.

[94] The building of API interfaces would be part of Phase 3 (Time & Material phase).

[95] The workflow for each of the category might vary. For example, the number of days after which the system generates a red alert for overdue or reminder before overdue.

[96] It is generally received in their office directly and not at the field audit office mail supervisor level.

the workflow relating to processing of the receipt is triggered and gets complete either when the status of the receipt is 'filed for information' or 'Response is sent'.

An actor must be able to monitor the status of processing of receipt by the actors who are reporting under. For example, the wing mail supervisor should be able to monitor the status of receipts of the entire wing. It is also important to note that in certain cases, the same communication may be received through various channels. For example, a receipt may be received through fax and e-mail. In such a case, the receipt is tagged under the same reference number. In few other cases, the receipt may be a duplicate version or a copy of earlier receipt. In such a case, the system should allow for clubbing of receipts for processing the same and mark as duplicate along with the link to original. The tracking of processing then happens through the original receipt.

It is important to note that any receipts received in person may also be uploaded as a receipt in OIOS system. This may be relevant for replies received during Apex Committee meetings, Audit committee meetings and joint sittings.

Indicative Business data relating to Receipts maintained by office mail supervisor

- Reference number (auto-generated by OIOS system)
- Letter number
- Letter Date
- Received from category (internal/external)
- Type of letter (C&AG, Named letter to HOD, Named letter to GO, Other, etc.)
- Language of the letter
- Status (Received, Transferred)

Channel of receipt

- Received from
- Received on
- Remarks
- Received through (In-person, regular mail, fax, e-mail, API[97], Web link[98])
- Attachments

Indicative Business data relating to Receipts maintained by wing mail supervisor / branch / section / dealing hand

- Nature of the letter: Look-up field with choices such as Response to IR paragraph, Response to SOF, Acknowledgement of intimation letter, Complaint, RTI, etc.
- Priority: High, Medium, Low
- Due date for response
- Status (Duplicate receipt, under process, Filed for information, Response sent)
- Link to dispatch, if the status is 'Response sent'
- Link to original receipt, if received as duplicate

Tracking details

- Remarks of the sender
- Sent to
- Sent on
- Carbon Copied to (In case, where response is needed from more than one wing/branch/section/dealing hand)

[97] In case of API these fields may be auto-filled.

[98] In case of web link, apart from the above fields, a reference number of the dispatch being referred may be auto-filled.

- Carbon Copied on (In case, where response is needed from more than one wing/branch/section/dealing hand)

45.1 Actors involved

The following are the actors involved in the maintenance of audit guidance document. The need for these roles can also be eliminated if the workflow is configured to reach the relevant personnel directly with Carbon Copy to the personnel in the hierarchy.

- **Office/Branch office mail supervisor** is the first point of contact for receipt generally and would be able to monitor the progress of processing of receipts for the whole office/branch office.
- **Wing mail supervisor** is an optional actor who will be able to monitor the progress of processing of receipts of the whole wing and is responsible for transferring the receipt to one or more relevant branches for processing.
- **Branch mail supervisor** is responsible for transferring the receipt to one or more relevant sections for processing and can monitor the progress of processing of receipts of the branch.
- **Section mail supervisor** is responsible for transferring the receipt to one or more relevant dealing hands for processing and can monitor the progress of processing of receipts of the section. The section mail supervisor may also initiate the processing of the receipt without passing it onto one or more dealing hands.
- **Dealing hand** is responsible for processing of the received receipt.

46 Dispatch (10_02)

This sub-module would provide a platform to send communication outside OIOS (internally within an office, to other field audit offices or branch offices within IA&AD or to entities that are outside IA&AD). The dispatch (multi-language) may be sent in various forms – paper-based communication; fax; e-mail; interfacing external systems. The sub-module will also assist in monitoring the progress of action taken on the receipt.

After the completion of processing of the receipt, it may be decided that the receipt may be ‘filed for information’. In such a case, no further action would be necessary. In other cases, a response would need to be sent to the sender of the receipt and others, wherever necessary. The preparation of draft of the dispatch to be sent may be done in a word processor or auto-generated by using a template stored in OIOS. The template would contain place holders for static text and image and dynamic fields which when used will generate a draft version of the reply automatically. This draft is then subjected to a workflow, where approval is sought from competent authority. The response may be ‘dispatched’ through various channels. Hence, the details regarding the same would be captured. In the case, where the response is dispatched via the regular mail, OIOS will track until the dealing hand / section completes the dispatch mechanism. The actual process of mailing from the office in this case is outside scope of OIOS. The possibility of integration with e-Post may also be explored.

Where the communication is paper-based, QR Code or similar machine-readable label should be considered to be part of the output.

The module should also facilitate the addition of a covering letter (in Hindi) and/or a translation of the text of the communication in Hindi.

Indicative Business data relating to dispatch

- Reference number (Auto-generated by OIOS)
- Language
- Remarks of the sender
- Link to receipt

Channel of dispatch

- Sent to
- Sent on
- Carbon Copied to
- Carbon Copied on
- Sent through (regular mail, fax, e-mail, e-Post, API[99], Web link[100])
- Attachments

46.1 Actors involved

The following are the actors involved in the dispatch sub-module.

- **Draft initiator** initiates the draft of dispatch (in few cases of miscellaneous generic letters) or auto-generates the dispatch based on templates (in most cases) and is responsible for completion of actual task of dispatch in case of regular mail, fax channels.
- **Reviewers** review the draft of dispatch and provide feedback.
- **Approver** is the competent authority to approve the draft of the dispatch.

47 Notification and alerts (10_03)

This sub-module would provide a platform for generation of notifications and alerts (configurable on various actions/ events within OIOS) through e-mail to staff within IA&AD as well as outsiders[101]. While, an alert is for information only, a notification would require the receivers to take action on the same. However, the system will track the action taken by the receivers by the task that was generated during the notification. During the technical design of each module, the notification and alerts required in the case of each module will be listed out. These notification and alerts are mostly generated by the system automatically. Hence, apart from the list of notification and alerts, the trigger for generation and set of receivers also need to be identified. Ideally, this needs to be a configurable feature as part of workflow engine. Apart from the above, the system must also provide for issuing a notification or alert manually to a group of receivers. The indicative business data relating to notification / alert is listed below.

Indicative business data relating to Notification

- Reference number
- Notification category (Reminder, Acknowledgement, etc.)
- Title
- Description
- Sent by
- Sent on

[99] In case of API, these fields may be auto-filled.

[100] In case of web link, apart from the above fields, a reference number of the dispatch being referred may be auto-filled.

[101] For example, periodical reminders requesting reply from the auditable entities. The communication to auditable entities through API interface to OCAMP system or state's IFMS is also another example.

- Sent to
- Link to workflow task that was generated during notification

Indicative business data relating to alert

- Alert type (‘Critical’, ’Warning’, ’Info’), colour coded/icons.
- Reference number
- Title
- Description
- Sent by
- Sent on
- Sent to

47.1 Actors involved

The following are the actors involved in the maintenance of audit guidance document

- **OIOS system** issues notification/alert based on workflow configuration and tracks task generated as part of a notification.
- **Receivers (internal)** are users who received a notification or an alert.
- **Senders (internal)** are users who manually issued a notification or an alert.

47.2 Activities envisaged in OIOS (for the module as a whole)

The activities (indicative) envisaged in OIOS are listed below.

- Receipts of inward communication through digital channels.
- Upload scanned communication received through traditional channels.
- Workflow for processing of receipt.
- Processing of dispatch (draft and annexures), both auto-generated and drafted.
- Outward communication through digital channels.
- Recording of outward communication through traditional channels.
- Configuration of generation of notification and alerts in a workflow or using a rule.
- Auto-generation of notifications and alerts.
- Monitoring of action taken on notifications.

11 ITA/PR/IW

The mechanisms of internal test audit, peer review and inspection wing are part and parcel of internal audit mechanism of IA&AD. The objective of all the three processes are the same i.e., to derive assurance on functioning of field audit offices or its wings/branches/sections (referred as 'clients'). This module facilitates planning, execution, reporting and follow-up mechanisms for the three processes. Since the processes or activities involved in ITA/PR/IW are very similar to the audit processes, the feasibility of reusing the appropriate business modules may be investigated.

48 T&M phase of ITA/PR/IW

The following sub-modules are envisaged in the time & material phase.

48.1 Internal test audit (11_01)

The internal test audit is done by a separate section within the field audit office. The internal test audit section directly reports to the HOD. They select and conduct audits of individual sections or branches within a functional wing in the field audit office. It is an activity that happens every year. This sub-module provides a platform to plan and execute internal audit of wings/branches/sections within a field audit office, issue and follow-up of internal test audit observations. The following activities are involved in the internal test audit process.

- Preparation of Annual / Quarterly audit plan and its approval (by HOD) containing list of sections to be audited.
- Scheduling of visits to sections.
- Request relevant records and scrutinise them.
- Issue enquiries to the section and receive response.
- Review response of the sections.
- Preparation and issue of report, after seeking approval from HOD.
- Submission of action taken report by the sections through functional wings of FAO periodically.
- Settlement of findings based on action taken by the sections.
- Periodical follow-up of the findings by competent authorities.
- Maintenance of related manuals and guidelines for easy reference.

48.2 Peer review (11_02)

Peer review is the process during which a field audit office is reviewed by peer-level officials on an assignment-by-assignment basis. A field audit office is not peer-reviewed every year. It may happen once in every three to five years. This sub-module provides a platform to plan and execute peer reviews of a field audit office, with a mechanism for follow-up by the concerned functional wing of C&AG Office. The following are the activities involved in the peer review process.

- Preparation of list of offices to be audited by Inspection wing.
- Nomination of peer review officer (proposal and approval) with approval from C&AG.
- Communication of nomination to the peer review officer.
- Communication of peer review officer to the field audit offices (For example, Annexure A, intimation of field visits).

- Communication of field audit offices to peer review officer (For example, filled Annexure A and other relevant documents/records).
- Documentation relating to relevant events (For example, Entry conference, Exit conference, etc.)
- Schedule of visit of peer review officer and team (may be sourced from multiple field audit offices) to field audit offices.
- Request relevant records and scrutinise them.
- Issue enquiries/draft report to the field audit office and receive response.
- Review response of the client.
- Preparation and issue of report, if necessary.
- Communication of peer review officer to C&AG HQ (Annexure B).
- Submission of action taken report by the field audit offices periodically.
- Periodical follow-up of the findings by functional wing of C&AG.
- Maintenance of related manuals and guidelines for easy reference.

48.3 Inspection wing (11_03)

A field audit office may be inspected by the IW once in every two to five years. Also, the inspection wing in the C&AG office also conducts inspections of field audit offices based on a theme. However, the periodicity of audit may also vary in the context of the selected theme. The following are the processes / activities involved in ITA/PR/IW. This sub-module provides a platform to plan and execute Inspections by the Inspection Wing in C&AG headquarters, with a mechanism for follow-up by the Inspection Wing and/or the concerned functional wing of C&AG Office.

- Preparation of annual audit plan and its approval containing list of field audit offices to be audited.
- Formation of team with members from wings in C&AG HQ.
- Schedule of visit to the field audit offices.
- Documentation relating to relevant events (For example, Entry conference, Exit conference, etc.)
- Request relevant records and scrutinise them.
- Issue enquiries to the field audit offices and receive response.
- Review response of the field audit offices.
- Preparation and issue of report. The report has findings under two[102] categories.
- Handing over of report for follow-up to the respective functional wings in C&AG HQ after a specified period of time.
- Submission of action taken report by the field audit offices periodically.
- Periodical follow-up of the findings by competent authorities (Inspection wing and functional wing in C&AG HQ).

[102] Category A, where the objections can be resolved internally by the office and Category B, where the resolution is dependent on external stakeholders for resolution. In case of Category A, the field audit office specifies the timeline required for resolution.

12 Knowledge Management System

The audit function of the IA&AD is a knowledge-based work. In IA&AD, Knowledge is an asset that helps in decision making and supports efficiency in planning and execution and adaptability in different audit assignments. Hence, knowledge must be deliberately created, consolidated and applied by the employees of IA&AD through a knowledge management system. Knowledge management provides for a means to share practices, expertise and learning across geographical boundaries. It reduces the risk of loss of critical knowledge which are retained by individuals.

The spectrum of knowledge in IA&AD ranges from judgement/intuition to documented/recorded knowledge. Thus, the KMS module of OIOS would need to provide a platform to share experience and insights and also to codify the knowledge as documented information.

In many organisations, Knowledge management system normally does not include data management (structured data). However, in the case of IA&AD, structured data of auditable entities form an inherent part of knowledge. Hence, KMS would involve management of structured, semi-structured and unstructured information. It should handle creating new knowledge, facilitating utilisation and application of current knowledge and handling outdated or invalid knowledge. It is important to understand the KMS module is only a means to knowledge management. It is also important to address the organisational culture and develop knowledge management enablers in order to achieve the outcomes of a KMS.

The sub-modules dealing with semi-structured and codified information are Audit Guidance, Auditee information system and media repository. The sub-module dealing with structured information is Auditee data warehouse, which does not form part of this RFP. KMS would also provide a platform for sharing of experience and insights through sub-modules wiki, forum and instant messaging.

49 Audit Guidance (12_01)

Audit guidance consists of documents that guides the employee about the procedures, instructions and methods relating to the various audit processes. The documents are applicable irrespective of subject matter of the audit assignment. For example, auditing standards. The guidance provided by the document may be mandatory or recommendatory in nature. The documents may become obsolete upon re-engineering of processes, standards, etc. of IA&AD. The objective of the set of documents is to clearly lay down the authority, duties and responsibilities of employees engaged in audit. In short, this module would replace the present practice of maintaining guard files in each and every individual field audit office.

The set of documents under audit guidance are hierarchical in nature. The hierarchy in this context means that sub-ordinate guidance document cannot over-ride[103] or *ultra vire* the superior guidance document. The document owner should verify and certify regarding the consistency of audit guidance document that the document intra-vires with higher-level documents. A QC certificate in this regard

[103] In case of deviation of lower-level guidance document from higher-level document, the same may be explicitly taken up for resolution. The resolution will result in either the higher-level document being amended or not allowing the lower-level guidance to deviate. This resolution would happen after seeking approval from competent authority.

would be uploaded in the OIOS system. The hierarchy information is maintained as levels[104] and document relationships in the sub-module.

The guidance documents may, in certain cases, also vary in their applicability. It ranges from constitutional provisions which are applicable universally in IA&AD to local circulars / orders issued in a specific field audit office and/or its functional wings. The following are the different document types that provide audit guidance.

- Audit mandate (Constitution, C&AG's DPC Act & Audit regulations) (Highest in the hierarchy)
- Auditing Standards
- Auditing Guidelines
- Auditing Manuals (issued by the C&AG HQ)
- Practice Guides and Guidance Notes (issued by C&AG HQ)
- Letters issued by C&AG HQ.
- Circulars / instructions issued by the Headquarters Office (centrally by PPG/ SMU Wing and by individual functional wings of C&AG HQ).
- Audit Manuals of Field Audit Offices.
- Circulars / instructions / branch orders issued by Field Audit Offices.
- Branch orders by field audit offices.
- Other applicable documents (Lowest in the hierarchy).
- Externally sourced guidance documents (not really part of the hierarchy).

OIOS would provide a platform to maintain these guidance documents, with version control, in KMS. These documents would be available to all relevant field audit offices and its employees.

The audit guidance may be prepared internally or externally[105] sourced as well. The process of preparation of the document would be outside the OIOS ecosystem. However, OIOS would provide a platform for feedback from stakeholders. The first feedback would be during draft stage. In draft stage, OIOS would provide a platform to host the draft version of the document and receive feedback from the relevant stakeholders. The second set of feedback would be after finalisation where stakeholders might communicate inconsistencies, request for clarification, etc. The indicative business data relating to audit guidance document has been listed below.

Indicative business data relating to General guidance document

- Document reference number (codified)
- Document type (Audit mandate, standards, guidance note, etc.)
- Link to classification schema of audit guidance
- Document owner (Name of the field audit office)
- Source of the guidance document (Internal, External)
- If source is internal, what is the level of guidance (Level 0, Level 1, etc.)?
- Nature of guidance (Mandatory, Recommendatory, Obsolete)
- If external, name of the organisation/external entity
- Date of creation
- Date of update

[104] Level 0 – Mandate; Level 1 – Standards; Level 2 – Guidelines; Level 3 – Manuals; Level 4 – Other instructions (mandatory); Level 5 – Other instructions (Recommendatory);

[105] ISSAI standards prescribed by INTOSAI, IndAS prescribed by MCA, etc.

- Date of obsolete
- QC certificate (including confirmation about hierarchical conformity)
- Key words (tags)
- Potential review date (The document owner fills this up after finalisation of the document so that OIOS can send an alert / notification to facilitate review process. This would also be driven by SOP laid out for document review.)
- Document references/related documents
  - Nature of relationship (Higher-level, annexure, External references, Replaced by (in case of document becoming obsolete), amendments, correction slips,)
  - Link to related document
- Document version history
  - Version number
  - Major / minor version[106]
  - Nature of version (draft / final)
  - Summary of changes made
  - Document
- Applicability (All or specific field audit offices or specific functional wings in specific field audit offices)
- Access control (Notification is issued to all relevant stakeholders upon a new updated version being available). The access control may be restricted in terms of relevant field audit offices.

49.1 Actors involved

The following are the actors involved in the maintenance of audit guidance document.

Application administrator is responsible for maintaining the master data relating to the audit guidance document such as document type, classification schema, etc.

Preparer is the person who is responsible for initiating the draft of the guidance document and amendments to the guidance document (i.e. maintaining the document), and assures the quality and consistency of the guidance document. The preparer is also responsible for appropriately classifying the document and attaching the keyword to the document to facilitate keyword search. The preparer is also responsible for responding to the queries / feedback / comments received on the document by the stake holders.

Approver is the person who is responsible for approval of the document and.

Stakeholders are the users who use the document. The provide feedback during draft stage and can request for additional details and clarifications. They must be able to search for the guidance document drilling down through the classification schema or perform a keyword / full-text search of the content.

49.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Administration of classification schemas.
- Searching the document using keywords.

[106] The major versions indicate significant changes are numbered as Versions 1, 2, 3, etc. The minor versions indicate lesser significant changes are numbered as Versions 1.1, 1.2, 1.3, etc.

- Performing a full-text search which searches the content of the documents.
- Browsing the classification schema to find the documents.
- Uploading of draft version of document.
- Receiving feedback for the draft version of the document.
- Uploading the final version of document.
- Maintenance of meta-data of the document.

50 Auditee IS (12_02)

This sub-module provides a platform for maintaining semi-structured/unstructured data relating to auditable entities. This would include documents (word, pdf), images, videos, csv files, Excel files, xml files, etc. It is important to understand that the owners of the data are external to IA&AD. The intention of the sub-module is to create a repository of auditee information and be available to be retrieved during a search.

The metadata that is stored for each data type may be different and hence need to be configurable. An illustrative list of fields for 'document' data type (and with role-based access control) is listed below.

The sub-module will provide the following types of search facilities.

- Searching for data using keywords.
- Searching the full content in case of documents.
- Browsing through the classification (illustrated in section below) and finding relevant data.

The population of semi-structured/unstructured data is based on data collection by employees of IA&AD. This happens either through specific data collection assignment or through data collection during an audit assignment. When any employee submits data along with relevant meta-data, an AIS manager would ensure that the data is relevant and that there is no duplication of data. The search tool would serve this purpose as well. Thus, meta-data tagging and search mechanisms would assist in avoiding duplication. The sub-module would also provide features for review and archiving of documents, when no longer needed.

50.1 Illustration for Taxonomy / classification schema for auditee information system

The auditee information system may be attached to multiple classification schemas. For example, Governance based schema, scheme-based schema or sectors/sub-sectors or accounting heads (six layered). The content of Auditee IS may be linked to more than one node in the classification schema. An example of a classification schema that would facilitate easy searching of auditee information would be the hierarchy of the auditable entities (in alignment with GoI directory), then drill and then further drilling down by activities / projects / schemes. An illustration is given below.

- Government of Odisha **(Government)**
-- Commerce & Transport **(Department)**
--- Motor Vehicle Department **(Sub-Department)**

1. Effective Public Service Delivery System **(Objective)**

1.1. Vehicular Pollution control **(Activity)**

2. Infrastructure development for enhancing the efficiency of transport administration and for improving citizen centric services **(Objective)**

2.1. To provide an efficient, Safe and Modern Transport Environment for people **(Goal)**

2.1.1. GIS Mapping **(Activity)**

2.1.2. Mobile apps for Bus Services **(Project)**

2.1.3. Permit Issue Management System **(Project)**

2.1.4. Inspection and Certification Centre **(Activity)**

3. Enhancing transport connectivity in the backward areas **(Objective)**

4. Establishment of Driving Training Institutes ensuring skill development **(Objective)**

4.1. Automated Driving Testing System **(Project)**

5. Enhancing road safety **(Objective)**

5.1. Road Safety fund **(Activity)**

5.2. Nirbhaya fund **(GoI Scheme)**

5.3. Installation CCTV camera in Public Transportation **(Project)**

6. Efficient collection of revenues **(Objective)**

Indicative business data relating to meta-data of data stored in Auditee IS

- Internal data reference number (codified)
- Data type (Document, Image, video, Audio, etc.,)
- Description of the data
- Review date for archive (The system would issue a notification for the data to decide on archival. During the initial upload, the AIS manager will set up a date based on SOP on retention policy in IA&AD. The policy creation and maintenance is outside the scope of the OIOS)
- If data type is ‘Document’, the following meta-data need to be maintained
    - Nature of document (Policy note, administrative reports, Government orders)
    - Document reference number (Issued by the document owner)
    - Document owner (Link to the auditable entity)
    - Date of document
    - Additional remarks
    - Document references
        - Reference type (Annexure, External references)
        - Reference document
- Keywords (tags)
- Classification to multiple to taxonomy/schema
- Other meta-data
- **Access control:** The access control[107] may be restricted in terms of relevant field audit offices.
- Linkage to audit assignments

50.2 Actors involved

The following are the actors involved in the maintenance of auditee information system.

Content contributors are responsible for sourcing the data that is to be stored in the Auditee Information System, uploading the data into the module and filling up meta-data.

[107] Some access rights are static, i.e., they don’t change over time. The access is permanently given to a user, groups of users, functional wings of FAO, field audit offices, etc. However, in respect of some documents, the access rights for some of the users would vary over time. For example, board minutes, agenda papers can be only be accessed by field audit team during a specific period of time, but will be accessible to Group officer of the functional wing of FAO permanently.

AIS manager is one or more persons in the field audit office and/or its functional wings who is responsible for approving the content to be uploaded into the AIS.

Stakeholders are the users who use the data. They must be able to search for the relevant data by drilling down through the classification schema or perform a keyword / full-text search.

50.3 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Uploading of the data by content contributors.
- Adding of meta-data to data by content contributors.
- Approval of meta-data and data by AIS manager.
- Issuing of alert regarding availability of new data regarding an auditee universe to all stakeholders.
- Receiving feedback on the draft version of the document.
- Uploading of the final version of the document and add meta-data for the document.
- Issuing of notification regarding the final version of the document.
- Receiving feedback / comments / queries on the final version of the document.
- Searching the document using keywords.
- Performing a full-text search which searches the content of the documents.
- Browsing the classification schema to find the documents.

51 Central repository of ADM/Tool kit (12_03)

The second set of documents are of specific in nature, which are applicable to a specific audit assignment. For example, audit check list, audit design matrix, etc. The classification schema for this central repository would be different.

The objective of the documents relating to specific assignments is to lay down the audit process for a specific audit assignment. For example, audit design matrices, checklists and audit tool kits of audit assignments would form part of the central repository. This sub-module would provide facility to publish the ADMs, checklists and tool kits relating to an audit assignment in the central repository. This repository may also include a link to audit findings or audit observations of the specific audit assignment. This sub-module would assist in sharing of experiences and knowledge in a specific subject matter of audit. The sub-module should provide a variety of ways (see below) for the employees to search for relevant material. Once the employee finds an ADM/checklist/toolkit useful, the system should allow pulling the guidance document into another audit assignment, where, it could be updated, if necessary and reused.

- Browsing through one or more taxonomy or classification schema.
- Searching through a keyword search.
- Full-text search of entire content.

The indicative business data relating to meta-data for content to be managed in Central repository is listed below.

Indicative business data relating to meta-data for content to be managed in Central repository

- Document reference number (codified)
- Document type (Audit design matrix, Audit checklist, Data collection kit)

- Document owner (Name of the field audit office or its functional wing)
- Date of publishing
- Categories in Classification schema (Multiple select)
- Remarks of the document owner
- Key words (tags entered by the Document owner)
- Link to audit assignment
    - Name of the audit assignment
    - Type of audit assignment
    - Field audit offices involved
    - Link to audit observations
- Access control (Notification is issued to all relevant stakeholders upon a new updated version being available). The access control may be restricted in terms of relevant field audit offices, wherever necessary.
- Average rating (from expert or leaders in Communities of Practice)
    - User
    - Remarks of the user
    - Average rating (across all parameters)
- Rating per parameter (The parameter should be configurable).
- Reuse history
    - Link to audit assignments which re-used/re-using the ADM/checklist/toolkit
        - Name of the audit assignment
        - Type of audit assignment
        - Field audit offices involved
        - Link to audit observations, if available

51.1 Actors involved

The following are the actors involved in the maintenance of audit guidance document.

Application administrator is responsible for maintaining the master data relating to central repository such as classification schema, etc.

Owner is the person who prepared the specific document which was utilised in specific audit assignments and who will set up access control.

Stakeholders -are the users who use the document. They must be able to search for ADMs/Toolkits/observations/audit products drilling down through the classification schema or perform a keyword / full-text search of the content.

51.2 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS are listed below.

- Administration of classification schemas.
- Publishing the content.
- Classifying the content and filling up meta-data, wherever necessary.
- Searching the content using keywords.
- Performing a full-text search.
- Browsing the classification schema to find the content.
- Pulling the content to re-use in a specific assignment.
- Giving feedback on the content.

52 Forum (12_05)

Provides a platform for informal group discussions based on subject matter of discussion, where instant response is not expected. The system integrator would provide a solution satisfying the following requirements.

- Segmentation of access: Not all employees need to have access to all discussion forums.
- Open user groups / Closed user Groups / Communities of practice
- Moderation of content and administration of groups (membership)
- Management of posts and threads
- Attachments
- Poll
- Event management
- Rich content
- Private messaging
- Email and SMS notifications
- Search engine: It should not only search the title, categories, and tags of a forums and its posts, but also index and search all of the discussion content itself.
- Favourites
- Auto-subscriptions
- Single sign-on / LDAP integration
- History

53 Wiki (12_06)

This sub-module provides a platform for a knowledge base, where the employees of IA&AD can modify the structure and content in a collaborative manner. Thus, this would provide scope for flexible content management system. This platform will thus help share audit experience in an informal manner. The system integrator would provide a solution satisfying the following requirements.

- Creating and linking pages
- Editing pages
- Navigation
- Searching (Title and full-text search)
- Classification schema
- Content moderation only with respect to present of offensive language and not accuracy / correctness.

54 Media repository (12_07)

This sub-module provides a platform to create, maintain and forward/circulate news digest manually and for advance web crawling/scraping/RSS feeds to create a media repository. The platform would provide facility for auto-classification in case of web crawling/scraping/RSS feeds. The system integrator would provide a solution satisfying the following requirements.

- Add/edit/delete content manually.
- Auto-addition of content based on Web crawling/scraping, RSS feeds.
- Auto-classification to multiple taxonomies based on logic.
- Hierarchy and sort order management

- Query / search / Filtering of searches
- Access control
- Import / export
- Life-cycle management (including Archival)
- Communication to relevant stakeholders.
- Trending / Popular searches.

55 T&M phase of KMS module

55.1 Instant messaging (12_08)

This sub-module would provide a platform for group discussions based on subject matter or area of work, where instant/near instant response is expected. The system integrator would provide a COTS solution satisfying the following requirements.

- Invite users
- Contacts (Integrate with directory of OIOS)
- Private messages to users
- Closed groups and admin
- Text messaging
- Attachment of images/documents
- Multi-language input
- Ability to search

13 Reporting/BI

The objective of the module is to provide a platform for self-serviced and managed service delivery of MIS reporting and dashboard for the information that is stored as part of OIOS. The system integrator should propose a COTS or OS solution for the MIS reporting and dashboard requirements. IA&AD requires a flexible and user-friendly platform. The solution architecture of this module should be designed in such a way that the performance does not impact regular transaction processing. So, separate reporting servers may be considered in the solution architecture.

56 MIS Reports (13_01)

56.1 MIS reporting on audit process data in OIOS

The management information system reports aid the managers at all levels in evaluating the activities of employees, make decisions and monitor progress. The IA&AD Department is presently achieving this by compiling various periodical returns and reports (mostly manually) and communicating to relevant stakeholders/managers at various levels. The reports are compiled at various levels viz., dealing hand, section, branch, wing, branch office, main office, field audit office (including both main office and its branch offices). Hence, it also involves consolidation of MIS reports of lower level to arrive at the MIS report at a higher level and this process is also predominantly manual.

Some MIS reports are reports where the information is extracted as on a particular date. Some reports behave like an account with opening balance, additions, clearances, and closing balance. Some reports require a time series analysis. Some reports need to be automatically generated in a periodical basis and available for viewing purpose. Others might be generated on an ad-hoc/on-demand basis.

While we expect SI to aid in preparation of a few complex reports (up to a maximum of 500 for Phases I and II), the solution should provide for a facility to create as many MIS reports are required on a sustainable basis. While, the common reports would be designed and deployed by the application administrator, the office/wing administrators can design and deploy reports that are specific to a field audit office or its functional wing. The user-interface for designing of the report should be very simple and user friendly[108]. When the design of a MIS report or periodicity is changed, a notification must be sent to stake holders.

Some reports must take parametric input (with filtering and sorting capabilities). The MIS reports must be viewable in the web and should be available for download as csv, Excel and pdf. When the MIS reports are viewed on web in a grid form, the solution should provide turning on/off visibility of columns, multi-sort, filter builder, grouping functionalities by simple clicks or drag and drops.

Some reports need to be built with hyperlinks (with click for details) and drill-down capabilities. The selection of input on a drill down acts an input parameter to the report. Some reports need summarization/pivoting capabilities and may be cross-tab queries. Some reports might require calculations to be made on fields.

The following are a **few** illustrations.

[108] The tool/solution should provide facilities to construct a query using GUI (For example, drag and drop). The solution should also allow to write queries in a SQL like language for complex queries

a) A report may be on number of auditable entities planned and audited for a field audit office. In this case, a report compilation team in every functional wing of FAO will first compile it for the wing. Then a central co-ordination team will consolidate the same details for the field audit office.

b) A report may be on outstanding paragraphs for the month with opening balance of previous month, additions in the current month, clearances in the current month and closing balance of the month. In the manual system, the report is first compiled by the dealing hand, then consolidated at section, branch and wing thereafter. This report needs to be runnable at various levels. In the OIOS system, this translates to record based permissions / access control as explained below.

Level	Record based permissions/Access control
Dealing hand	Can run the report at his level.
Section	Can run/filter the report individually for each dealing hand reporting under or for the section as a whole.
Branch	Can run/filter the report individually for each dealing hand or each section reporting under or for the entire branch as a whole
Wing	Can run/filter the report individually for each dealing hand or each section or each branch reporting under or for the entire wing as a whole.

c) A report on number of working days spent by each employee on each activity in an audit assignment. The audit fee, if due, is calculated based on the number of working days.

d) A report listing the list of outstanding paragraphs from previously issued inspection reports.

e) List of records not produced during an audit programme, during a year by an auditable entity and entities reporting to it, by an auditable entity across time.

f) A report which picks a specific number (say 5) of inspection reports which were issued during a month randomly.

The system should provide for arranging the MIS report (the ones prepared by IA&AD) in a menu/sub-menu wise, as desired by the administrators. The administrators should also have the ability to define access control for the same. The solution should allow for maintenance of meta-data for each report. The indicative business data is listed below.

Indicative business data for MIS reports on process data

- Reference code
- Name of the report
- Description of the report
- Type of MIS (Periodical / On-demand)
- If type is periodicity[109],
  - What is the periodicity (Daily, Weekly, Monthly, Quarterly, Semi-annually, Annually)?
  - What is the start date?
- Created by
- Created on

[109] Although periodicity is not necessary, it may be useful as a transitional measure and also to send to external stakeholders.

- Access rights
- History of update on design (Notification is sent to stakeholders after update)
  - Updated by
  - Updated on
  - Remarks during update
- History of running of report
  - Reference number
  - Summary of values of parameters used
  - Run by
  - Run on

56.2 Actors involved

- **Designer** (Application/office/wing administrators) designs the MIS reports, fills the meta data, provides access rights and publishes in the system
- **Approver** of the design of the MIS report, if necessary.
- **Stakeholders** who have access to run the MIS report/data extract, view the data and download it.

56.3 Activities envisaged in OIOS

The activities (indicative) envisaged in OIOS is listed below.

- Design a MIS report.
- Review the design of MIS report.
- Approve the design of MIS report.
- Publish a MIS report to repository at various levels (functional wing of FAO, field audit office, IA&AD) so that it can be used by others.
- Allocate access control to a MIS report.
- Run a MIS report.

56.4 Dashboards (13_02)

Dashboards are user interfaces which provides indicators relevant to a particular activity or objective. It visually presents the indicators / measures and consists of multiple reports. It is also interactive and helps the user to play around and view the indicator information as much as he wants. It includes interactive visualisations with ability to produce infographics (For example Geographical heat maps). The system integrator would assist in identifying an appropriate COTS solution with necessary features. The design and development of dashboards is done by the designers, who will deploy the dashboard onto the OIOS application. The following functionalities are required. The same tool needs to be flexible enough to be used for preparing visualisations as part of interactive digital reports.

- Mobile ready
- Web based
- Real-time data feed
- Easy visualisation with drag and drop editing.
- Automated data refresh
- Design / build dashboards
- Publication of dashboard
- Access control

- Alert and notifications
- Drill-down interactions (Granular view)
- Access control (per user or user groups)
- Meta-data (Name, description and category)

56.5 Actors involved

- **Designer** (Application/office/wing administrators) designs the dashboards, fills the meta data, provides access rights and publishes in the system
- **Approver** of the design, if necessary[110].
- **Stakeholders** who have access to view the dashboards.

56.6 Activities envisaged in IT platform

The activities (indicative) envisaged in OIOS are listed below.

- Design a dashboard.
- Review the design of dashboard.
- Approve the design of dashboard, wherever necessary.
- Publish a dashboard to repository at various levels (functional wing of FAO, field audit office, IA&AD) so that it can be used by others.
- Allocate access control to a dashboard.
- View and interact with a dashboard

[110] Standardized reports required such as for HODs and Group Officers.

14 Technical Guidance & Support

The accounts of the Panchayati Raj Institutions (PRIs) and Urban Local Bodies (ULBs) is audited by Local Fund Auditor (LFA). The LFA, is generally an officer of the State Government, except in the states of Bihar, Jharkhand and West Bengal, where the LFA is an officer of the C&AG. The LFA is responsible for audit of PRIs and ULBs. In cases where LFA is an officer of the State Government, C&AG provides Technical guidance and support (TGS) (where entrusted by the State Government) to audit of PRIs and ULBs.

The role of the C&AG and the field audit offices of IA&AD to provide TGS to such audit by the Examiner/ LFA, is detailed in Chapter 10 of the Regulations on Audit and Accounts, 2007 (https://cag.gov.in/content/regulations-audit-accounts-2007#chapter10). This module will provide a platform to provide TGS for audit by Examiner/ Local Fund Accounts of PRIs and ULBs. However, normal audit of ULBs and PRIs, where covered elsewhere under the C&AG's audit mandate, will be covered under the normal Audit Planning, Audit Execution, and Audit Reporting etc. Business Modules. The module would be implemented completely in the time & material phase.

57 T&M phase of TGS module

The following sub-modules would be implemented in the time and material phase.

57.1 TGS (14_01)

This sub-module would provide a platform for Technical Guidance and Support (TGS) of Audit by Examiner/Local Funds of PRIs and ULBs. The following processes would be captured in the OIOS.

- The inclusion of local fund auditors (in states other than Bihar, Jharkhand and West Bengal) as users of OIOS may be considered.
- Receipt of the annual audit plan of LFA and capturing the same within the system.
- Provision of comments on the draft manuals, guidelines and guidance notes and capturing the final version along with meta-data in the system.
- Maintenance of list of inspection reports of audits conducted by the LFA and a copy of the report attached to the same.
- Scrutiny of selected inspection reports issued by the LFA for monitoring their quality.
- Monitoring of the activities of the LFA through received returns submitted by the local fund auditor through the '**10: Communication module**'.
- The test-checking of some PRIs and ULBs and preparation of Annual technical inspection report (ATIR) containing the findings of audit of PRIs and ULBs would be performed through the Audit Planning, Audit Execution, and Audit Reporting modules. The ATIRs may be submitted to the respective state legislatures.
- Conduct training and capacity building of the staff of LFA.

57.2 LB Committee follow-up (14_02)

This sub-module would provide a platform to implement Legislative LB Committee follow-up process of LB audit reports, similar to the process followed by PAC/ COPU for other Audit Reports.

15 Administration (Non-HR)

This module deals with non-HR functionalities of administration. The HR related activities are handled in ‘**02: Personnel module’**. All the sub-modules are to be taken up during Time & Material Phase. These sub-modules may be considered as ‘last mile connectivity’ modules in the journey of OIOS.

58 T&M Phase of Administration (Non-HR) module

The following sub-modules are proposed to be taken up during Time & Material Phase.

58.1 Office procurement (15_01)

This sub-module would assist in managing procurement processes of an office/IA&AD. The actual procurement is done predominantly through the Government e-Marketplace (GeM) application. This would be out of scope of OIOS. However, the following would be within the scope. An integration with PFMS may be considered. The following features are envisioned in the sub-module.

- Workflow of internal processes involving proposal for procurement (product / services / projects), administrative approvals and financial approvals;
- Documentation relating to procurement. For example, contracts;
- Process relating to O&M of the procured goods and services (integrated with the asset inventory sub-module);
- Disposal mechanisms (integrated with the asset inventory sub-module).

58.2 Asset management (15_02)

This sub-module would assist in managing information relating to assets (movable and immovable) of an office. The immoveable assets include office and residential buildings (owned/rented by field audit offices of IA&AD). The moveable assets include (not limited to) furniture, fire safety, books[111], subscription to digital assets, IT equipment, etc. OIOS should aid in maintaining a link between related assets. For example, furniture in an office building of a field audit office. OIOS should also aid in maintaining attachments relating to assets. For example, maps, floor plans, title deed, drone videos of office premises of a field audit office.

The following features are envisioned in the sub-module.

- Tracking of all assets centrally (The ITSM solution may be in existence and running when this sub-module is taken up for design and deployment. Hence, the design of the sub-module should be taken after due consideration of ITSM capabilities).
- Asset tracking throughout the lifecycle including move, add, change and delete (MACD) activities (Integrated approach with procurement sub-module).
- Maintenance of meta-data including (not limited to) asset type, ownership (owned, rented, etc.,), link to other assets, attachments, allocation information[112], status[113].
- Tracking of service and maintenance contracts (Integrated approach with procurement sub-module)

[111] If required, a separate library management sub-module may be considered.

[112] For example, Allocation of residential quarters to employees.

[113] Status would vary for asset type and sub-type. For example, the status of assets of type ‘Residential’ under immoveable assets would have a status of ‘Occupied’, ‘Vacant’, ‘Under maintenance’, ‘Under renovation’, etc.

- Audit of Asset data and tracking of existence.
-

58.3 Inventory management (15_03)

This sub-module would assist in managing inventory relating to consumables (IT consumables, Paper and stationery, Office supplies etc.) of an office. The following features are envisioned in the sub-module.

- Single view of inventory with what is in stock, in transit and current demand levels[114] (with alert mechanism for re-ordering and maintaining minimum order levels).
- Indents and processing of indents.
- Monitoring of receipt of stock in-terms of time of delivery and cost.
- Measure performance of vendors.

58.4 RTI (15_04)

This sub-module would assist in managing process of receipt and response to applications received under the Right to Information Act, 2005. OIOS should facilitate compliance to provisions of RTI Act, 2005. The following features are envisioned in the sub-module. This sub-module may be used by the field accounts offices as well.

- Definition of roles of Appellate authority (AA), Public Information Officer (PIO) and Assistant Public Information Officer (APIO) in OIOS.
- Linking of specific posts to the roles of AA, PIO and APIO.
- Receipt of RTI application (optional) (The feasibility of online receipt may be studied when this sub-module is undertaken). The exact date of receipt is an important criteria for timely action under various sections of RTI Act, 2005.
- Capture of details of the received RTI application.
- Transfer of the application to another external office (not within the field audit office), where felt necessary under Section 6(3), within the stipulated time in the RTI Act (OIOS should raise a warning alert). In case of transfer, the clock with stipulated time to reply to the RTI Act is reset.
- Details regarding communication with third party, wherever necessary.
- Configure the workflow to send the RTI application to relevant field audit office / wing / branch / section and receive responses from them.
- Monitor disposal of RTI applications within time by tracking of RTIs and red alerts for priorities.
- Appeals to RTI applications.
- Details of CIC cases and hearings attended for a specific application including attachments (notice), dates of hearing, report by attendees and status. OIOS would not capture the process but only the data.
- A link to the RTI Act, 2005 and its amendments for easy reference.

58.5 Complaints (15_05)

This sub-module would be managing process of receipt and response to complaints received at various offices. This sub-module may be used by the field account offices as well for complaints/grievance redress.

[114] Current demand levels are for specific type of consumables, such as ‘IT consumable’.

- Receipt of complaint[115] (The feasibility of online receipt may be studied when this sub-module is undertaken). Interface with CPGRAMS[116] may be considered for e-receipt of complaints/grievances.
- Capture of details of the received complaint.
- Configure the workflow to send the complaint to relevant field audit office / wing / branch / section and receive responses from them.
- Ability to forward the complaint to relevant field audit teams, in case where a field verification is necessary.
- Monitor disposal of complaints.
- Forwarding of a complaint as an additional audit insight, wherever necessary.

[115] Integration with '**10-Communication module**'.

[116] Centralized Public Grievance Redress And Monitoring System.

16 Legacy data

59 Overview

In order to ensure business continuity of the activities of IA&AD, in the same platform (OIOS system), it is essential to migrate legacy data, wherever relevant. This module details out of the To-be process for legacy data migration. OIOS is expected to provide a platform for smooth migration of legacy data.

A common policy enlisting the principles and requirements regarding migration of legacy data needs to be laid out. This policy is solely for internal purposes and will not be part of RFP. The policy would be forwarded for consideration of PPG group for perusal and approval and communication as part of 'Change management policy for on-boarding to OIOS'. The following are the principles/assumption governing migration of legacy data.

59.1 Principles/Assumptions governing legacy data

The rollout of OIOS system in a field audit office or its functional wing is independent of migration of legacy data. Any MIS report being generated by OIOS would include only data that is part of it. Therefore, the reports would not reflect complete position of the field audit office.

A handshake would be made on the data elements or groups of data elements for which the module should facilitate legacy data migration (including attachments and the naming conventions). The same has been indicated in each module individually. The fields that would be filled mandatorily for each entity, for the purpose of data migration, would also be mutually agreed upon. A data migration design document would be prepared to reflect the same. A set of Excel templates would be drawn reflecting the data migration design and distributed to field audit offices to facilitate bulk data migration. A data migration guide / user manual that assists the field audit offices to fill the Excel templates would also be distributed. It is relevant to note that OIOS may store more fields for an entity than the fields agreed upon for data migration.

Further, the legacy data might have missing data elements including referential integrities. For example, the employee master data may not have details regarding employees who had retired. Thus, when it comes to migration of data relating to the audit observations, if the employee who raised the audit observation had already been retired, and the employee master data does not have the master record, the reference relationship would be missing in the data migration. The platform must be able to accept and handle this situation. The solutions for handling the missing elements and reference relationships would be part of the data migration design document and the same would be incorporated in the Excel template.

The OIOS system should treat data elements that were created as part of workflow and data migration equally for reporting purposes. For example, when the user is trying to list audit programmes relating to an auditable entity, the audit programmes created using workflow of OIOS and the legacy data migration must be displayed.

The SI is not responsible for digitisation of the data but is responsible for offering the following ways through which data migration is facilitated.

Data migration includes both meta-data and related documents/attachments of the entity.

59.2 Current vision for data migration

The current vision with regard to migration of legacy data under each relevant sub-module is detailed below.

Ref #	Sub-module	Data migration requirement
01_01	Office master	The legacy information regarding offices are currently maintained in a FoxPro database and Excel maintained by an external developer. The same will be migrated into OIOS.
01_02	Office structure	The information is not stored in an electronic application in most of the offices and the scope for data migration is minimal. However, the same are stored in home grown applications in the IA&AD. The feasibility of migrating the data may be explored.
01_03	Privilege master	No legacy data migration is necessary as this is immutable master prescribed by the System Integrator.
01_04	User roles	No digital legacy data is available. The information needs to be entered by the field audit offices.
01_05	User role-office structure mapping	No digital legacy data is available. The information needs to be entered by the field audit offices.
02_01	Employee master	The employee details are available in various databases. These details have to be collected and migrated into OIOS as much as possible. Upon migration from legacy databases/data entry, the same may be validated by the employee as a one-time measure.
02_02	Employee profile	The employee details regarding qualifications, certifications, examinations are available in various databases. These details have to be collected and migrated into OIOS as much as possible. Upon migration from legacy databases/ data entry, the same may be validated/ confirmed by the employee.
02_03	Employee posting	The employee details are available in various databases. These details have to be collected and migrated into OIOS as much as possible. Upon migration, the same may be validated by the employee. It is important to capture the present posting of employees even if legacy data is not migrated.
02_04	Nominations for training / capacity building	The previous training nominations are available across various databases which may be brought into OIOS, as much as possible. Upon migration, the same may be validated by the employee.
02_05	Other administrative nominations	There are no standard databases or datasets available for nomination of employees for administrative activities.
03_01	Auditee universe	The auditee universe details are available in various databases. These details would be collected and migrated into OIOS as much as possible; further changes after the migration should be processed only through OIOS.
03_02	Auditee universe profile	The field audit offices will feed the profile data relating to the auditable entities themselves. A mass data migration is not feasible in this regard.
04_02	Annual audit planning	The data migration of legacy plans is not envisaged. The preparation of annual audit plans of IA&AD in OIOS is envisaged to begin from 2020-21.

04_03	Parametric risk analysis	No migration envisaged.
04_01	Strategic audit plan	No migration envisaged.
05_01	Sampling approach	No migration envisaged.
05_02	Audit design matrix	The legacy audit design matrixes may be uploaded in the central repository for reference.
05_03	Audit guidelines	The legacy audit guidelines may be uploaded in the central repository for reference.
06_01	Audit programme	Minimal data about legacy audit programmes to the extent necessary (e.g. for units planned earlier, but audit being executed through OIOS) would be migrated.
06_02	Record requisition	Nil
06_03	Audit enquiry	Nil
06_04	Audit observation	Audit observations pending settlement from previous audits may need to be migrated. The extent of legacy migration would be decided individually by each field audit offices. Some field audit offices have digital data in Excel, Access or in an IT application. Some field audit offices do not have digitized records. The digitization of the records to mine the legacy data would be the responsibility of the individual field audit offices and not that of the system integrator. However, depending upon the design of the data structure for OIOS, the missing references need to be filed in by default based on a logic. For example, the concept of 'assignment' does not exist in pre-OIOS era. So, if the data structure flows as assignment -> programme -> audit observations, then logic of filling up assignment level fields (only minimal) need to be built in the data migration design.
06_05	Audit Toolkit (Collect)	No data migration envisaged.
07_01	Configuration of audit products	The existing configurations would be added in the OIOS.
07_02	Drafting an audit product	No data migration envisaged.
07_03	QA/QC within field audit office	No data migration envisaged.
07_04	Finalisation and issue	The data migration in each type of audit product would be decided by the field audit offices. **Inspection reports** The facility to migrate data relating to previously issued inspection reports in which the audit observations are still pending needs to be provided by OIOS. **Audit reports** The legacy audit reports, to the extent necessary, have to be migrated into OIOS and be available as part of OIOS.

		Previously issued audit certificates No data migration envisaged.
07_05	Receive response	The response to legacy audit products (which are still not yet closed) may need to be migrated into OIOS.
07_06	Recommendations	No data migration envisaged
08_01	IR/DAN follow-up	Though, the legacy data relating to response of the auditable entity to audit observations are available, the field audit offices can choose to migrate one of the following. a) No data migration which means processing of replies from a specific date through the system. b) Data migration of replies pending processing. c) Latest reply for all audit observations that are pending. d) All the replies for all audit observations that are pending. e) b), c) or d) above but for legacy data for a specific period of time.
08_02	PAC/COPU/Other LC follow-up	The data relating to pending Explanatory Notes, ATN/ATRs and pending PAC recommendations have to be migrated.
09	Data collection module	No data migration is envisaged.
10	Communication	No data migration is envisaged.
12_01	Audit Guidance	The existing data / documents may be migrated into the OIOS systematically.
12_02	Auditee IS	The existing data / documents may be migrated into the OIOS systematically.
12_03	Central repository of audit design matrix and audit toolkits	The existing data / documents may be migrated into the OIOS systematically.
13_01	MIS reports	The existing periodical and adhoc returns need to be designed in the solution for each of the business module.
13_02	Dashboards	No data migration is envisaged.

60 Bulk data migration service (16_01)

OIOS should have feature to offer bulk data migration service. The field audit offices would be responsible for capturing details of entities in prescribed formats (Excel). Then, the field audit offices then request for a bulk data migration service through a specific web-page by filling in a form and uploading the Excel files (containing data) and the zip[117] files (containing attachments). The 'Data migration support team' of IA&AD would then load the Excel files(s) into the 'Validator' of OIOS to ensure that the data to be uploaded is valid. If there are any validity issues, due to any reason[118], the same is notified to the field audit office. The interaction between the field audit office and the 'Data migration support team' of IA&AD goes back and forth until the data validation is successful.

[117] An unzipping facility must be provided as part of the data migration platform, if the uploader wants to view the files in the zip file.

[118] Primarily data becomes unfit to be uploaded because the data does not pass the input validation control tests such as null data for mandatory fields, mismatch in data types, failure in master data validation, etc.

Once the data validation is successful, the data is passed on to the System Integrator's migration team so that the data can be loaded into OIOS. The interaction between the 'Data migration support team' of IA&AD and the SI's migration team goes back and forth until the data migration is successful. A turnaround time and max number of iterations (for purpose of costing) would be fixed as part of SLA.

The field audit offices should be able to verify the status of the request at any point of time. The ticket for the requested service gets finally closed upon successful migration of the data.

60.1 Migration of data from existing IT applications

Some of the field audit offices have existing IT applications which are being used to store audit process data. The legacy data to be migrated would be exported into Excel file in the prescribed formats. Then, the field audit offices would use the bulk data migration service to migrate their data.

61 Ad-hoc entry of legacy data (16_02)

The field audit offices would also need a mechanism to enter one-off records which were missed during the initial data migration. Also, a field audit office might choose not to use the bulk data migration service but rather prefer to the data entry in the system by themselves. Hence, OIOS should provide for a facility with necessary forms (containing the fields of the entities and facility to upload the attachments) so that the data could be entered.

62 Appendix I - Modules that are NOT IN SCOPE

This module is NOT IN SCOPE for the RFP. The high-level details are being placed here so that the System Integrator has an understanding of the module and potential implications on the design of other modules/sub-modules.

62.1 Auditee data warehouse / lake / hub with data analytics (12_04)

The first objective of the module is to provide a platform for warehousing the structured data of auditee, viz., financial information, accounting information and transactional information. This structure data is utilised by the field audit offices throughout the audit processes such as audit planning, audit execution, audit reporting for various purposes. The field audit offices would perform data analysis on the relevant data available in the data warehouse in order to perform the following activities.

Process	Activities which would utilise the data available in the data warehouse
Audit planning	• Selection of subject matter under each audit assignment. • Assessment of risk for identifying focus areas in the selected subject matter. • Selection of auditable entities to be covered for each audit assignment. • Selection of a sample of transactions of auditable entities to be covered under each audit assignment.
Audit execution	• Identification of red flag transactions which poses audit risk. • Testing of controls for regularity. • Testing of transactions for compliance. • Analysis of data collected to arrive at audit observations and conclusions.
Audit reporting	• Visualisation of audit findings. • Preparation of interactive digital reports. • Preparation of MIS reports that assist in decision making. • Preparation of dashboards that assist in continuous monitoring.

This sub-module would provide a platform for both data management and data service delivery. The requirements for both the processes are described in detail below.

62.1.1 Data management

The process of data management includes data collection, ETL processes (wherever necessary), warehousing the data and archival. The process of co-ordinating with the auditee, signing protocol agreements, designing API interfaces is not within the scope of the OIOS project. It would be taken up independently as mission mode projects. The expectation from the System Integrator is to provide a solution architecture for the business requirement discussed below.

62.1.1.1 Principles governing data management

The following are the basic principles that should govern the solution architecture that is to be proposed by the system integrator.

Confidentiality

The data that is being collected and stored as part of this sub-module is actually owned by the auditable entities. Hence, it becomes extremely important for C&AG to ensure the confidentiality of the data that is collected from the auditees.

Integrity

As explained in the above section, the data collected would be used in various audit processes. Hence, data integrity affects various aspects such as credibility of audit observations, accuracy of audit conclusions, etc. depending on the utilisation. While, the solution cannot ensure data integrity at source, the solution ensure data integrity during transmission and processing of data.

Availability

The data managed as part of this sub-module need to be available to the employees (based on access control logic). The solution should also provide facility to restore the data in case of any physical or technical incidents.

Hence, the solution architecture should consider the following security requirements.

- Ensure confidentiality, integrity and availability for the business requirements mentioned above.
- A balance between state of the art and cost of implementation.
- Restore access and availability in a timely manner in case of a physical or a technical incident.
- Appropriate to specific circumstance of IA&AD and the risk.
- Use pseudonymisation and/or encryption for personally identifiable information.
- Ability to perform regular testing, assessing and evaluating the effectiveness of solution.
- Protection against unauthorised or unlawful processing, accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
- Facilitate implementation of access control logic and two-factor authentication/biometric authentication

62.1.1.2 Data collection

The mode of collection of data from the auditable entities would be different. The following modes have been in practice.

File Transfer: Auditable entities provide data in csv, txt, Excel, JSON, XML Formats. The data in the files need to be loaded into the warehouse (with or without ETL).

Data dumps: Auditable entities provide data in the form of database dumps from their database (Oracle, Microsoft SQL Server, PostgreSQL, MySQL). The solution should facilitate restoration of these dumps without affecting the integrity of data and dependencies.

API Interfaces: A few auditable entities also provide data through API interfaces. This requires development of a package to extract information and store it in the warehouse. However, as specified earlier the development of the package is not within the scope of the Project.

62.1.1.3 ETL process

Depending up on the mode of data collection, the warehouse administrator / data manager of IA&AD might need to perform an extract, translate and load before warehousing. The solution should provide for an ETL platform which adheres to principles defined for data security in the previous section.

62.1.1.4 Warehousing

The solution should include a warehousing solution or an alternative to store the data in a meaningful structured manner with meta-data attached to it. Such warehousing should also facilitate cross-linking of data collected from various sources. The solution should also provide the facility to prepare and maintain documentation regarding the structure of the data warehoused including tables, columns, indexes, stored procedures, views and dependencies (As automatically as possible with a provision to add user-friendly remarks wherever necessary to assist data analytics). The indicative business meta-data is listed below.

Indicative business meta-data for data that is warehoused
Name of the data
Description of the data
Classification schema (Many to many)
Department / Auditable entity
Mode of collection (FT, DD, API)
Required (ETL)
Link to documentation
Review date for archival (This is set during warehousing and during subsequent review, so that the solution can send a notification for review to the administrator)
Reasons for continuance beyond the review date
Attachments (Protocol documents

62.1.1.5 Archival

Data archival is an important activity to ensure continued validity and relevance of the structured data stored in the data warehouse. It will also help in optimising resource utilisation and to prevent uncontrolled growth of the warehouse. The solution should help implement archival policy by sending notification to the administrator to periodically review and archive the data.

62.1.2 Data service delivery

The second objective of the sub-module is to provide services relating to data. These services should be delivered on a platform which provides access control, single sign on / integration with LDAP. There are two services the solution should facilitate delivering to the employees of IA&AD. These services would be performed through a basket of BI tools which would be able interact with the data warehouse and facilitate analysis and analytics.

- **Data extracts:** These are extraction of data from one or more sources in csv, Excel, xml, json, etc. These data extracts may also be performed by directly running a query for set of restricted users (For further details see below).
- **Interactive dashboards:** These are interactive dashboards created through the basket of BI tools available for the user.
- **Data analytics app:** These will assist in building common analytics within audit stream and analytics for assignments which are repeated over time (For further details see below).

62.1.2.1 Data extracts

The system should provide for creation of the extract, filling up meta-data, providing access rights to necessary stake holders and hosting the same. The data extract must be viewable in the web and should be available for download as csv, Excel, xml, JSON, etc. When the data extract is viewed on web in a grid form, the solution should provide turning on/off visibility of columns, multi-sort, filter builder, grouping functionalities by simple clicks or drag and drops.

Indicative business data for data extract on auditee data

- Reference code
- Name of the data extract
- Description of the data extract
- Classification schema (Many to many)
- Keywords
- Data sources used for data extraction
- Link to design file (query or otherwise)
- Documentation of data extract process
- Created by
- Created on
- Access rights
- History of update on design (Notification is sent to stakeholders after update)
    - Updated by
    - Updated on
    - Remarks during update
- History of usage
    - Reference number
    - Downloaded by
    - Downloaded on
    - Link to audit assignments which use it

62.1.2.2 Data analytics app

This module will help in employing embedded analytics to build a data analytics app. These apps are especially useful in two scenarios.

a) Audits which are repetitive in nature.
b) Audits which are common to audit streams in IA&AD.
c) Audits where there is a need for a time series for audit process data, i.e., there is a need to assess the subject matter in the exact manner after a period of time (Follow-up).

The responsibility of the SI is to assist in identifying suitable solution with the required features considering cost and overall OIOS ecosystem.

Illustration of use cases for possible analytics app

- Audit of implementation of MGNREGA by building an analytics app on MGNREGA.
- Functional area wise analytics app for auditing assessment, levy and collection of GST data.
- Analytics app for audit of administration of Income Tax, Customs, etc.
- BI Models for analysing PFMS/IFMS data.
- Analytics app for Vahan-Sarathi data.
- Audit of implementation of SDG targets.

The necessary requirements for the solution are listed below.

- API-first design
- Developer tool-kit for building data analytic apps
- Deployment of data analytic apps in an integrated manner with single sign-on / LDAP integration.

- Access control
- Integration with a workflow engine
- Scalability
- Governance of apps
- Robust security
- Meta data

The data service delivery solution should provide facility to host/deploy these services, maintain meta-data for the services, implement access control, classify based on a taxonomy/classification schema, parametric search (with filtering), keyword search and notifications/alerts.

The service delivery should support both self-servicing (data extracts and interactive dashboards created by field audit offices themselves) and centralised managed servicing (data extracts and interactive dashboards created by a central administration team). The principles of data security apply for this objective as well.

62.1.3 Actors involved

The following are the actors involved.

- **Warehouse administrator** is responsible for implementation of data management policy, protocol and maintain classification schema.
- **Data managers** are responsible for periodical testing of security.
- **Data Analysts** in field audit offices would use self-service mechanism to perform data analysis.

Comptroller and Auditor General of India

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Request for Proposal

`Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

'One IA&AD One System' (OIOS) Project

VOLUME – I – Annexure B

Reference Number: 51-ISW/2019-'One IA&AD One System' Project

Page Intentionally Left Blank

1. Contents

1. Introduction

This document provides envisaged indicative Architecture for OIOS Application. It also provides Solution Architecture overview.

1.1. Key Assumptions

Following key assumptions need to be taken care while designing OIOS architecture:

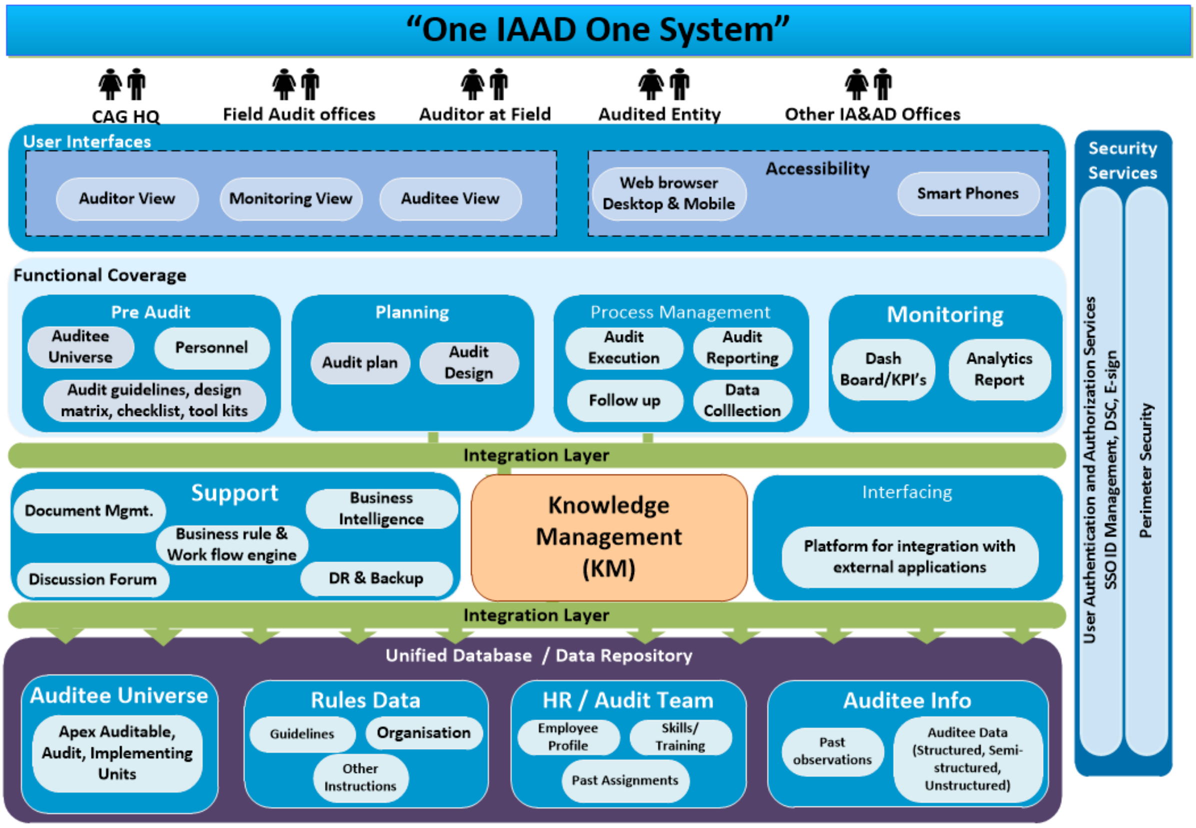
1. Government Process Re-engineering opportunity: OIOS application is a transformational opportunity. It is critical that the design is configurable for changes in next decade rather processes in past.
2. Adoption to evolving technology: It is essential that entire system is built to be open (standards, open API), component coupled loosely to allow changes in modules/ sub-modules without affecting other parts.
3. Ability to select best product at best rate as and when required: Architecture should be open, use commodity hardware, have NO vendor lock-in and designed for horizontal scalability.
4. Multiple device access: Access devices and their screen considerations (including browser variations) are numerous and constantly evolving; hence the design should provide adaptability.

The envisaged OIOS Application Architecture is covered as following:

1. Functional Architecture
2. Application Architecture including Data Architecture
3. Technical Architecture
4. Security Architecture

2. Functional Architecture

A high-level future One IAAD One System logical Architecture is depicted in the schematic below:



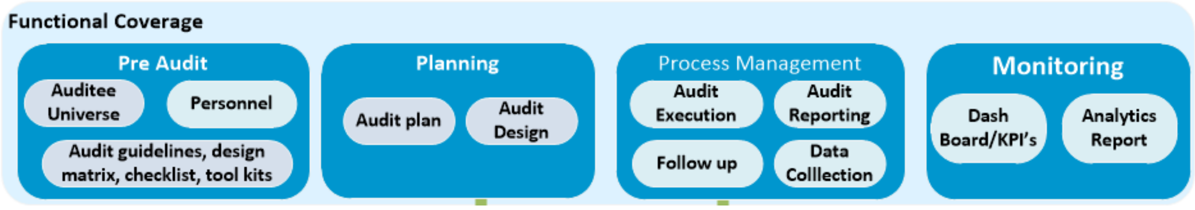
The Logical Architecture is a conceptual model depicting the enterprise architecture of the new centralized portal and application modules. It consists of following layers, namely:

1. Layer 1: **Users Interfaces**– The user layer comprises of the various users involved in Audit life cycle & support activities.

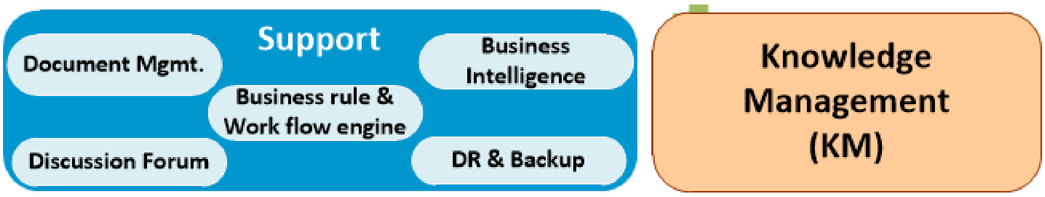
2. Layer 2: **Accessibility** – This layer comprises of the various interfaces/ channels that would allow the users to access one or more services/ applications. There shall be a single point of access for related functions that the user intends to use. Functionalities available for accessibility through smart phone may be limited as given in Vol 1 of this document.

3. Layer 3: **Applications**- This layer refers to the spectrum of applications which will be used to serve the needs of implementing paperless environment and to give enhanced services to all

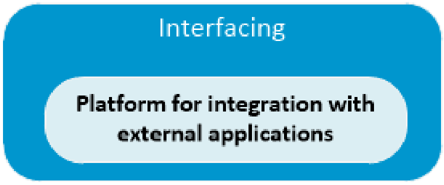
the stakeholders on secured, reliable and transparent environment. These applications would be supported on various platforms, including mobile.



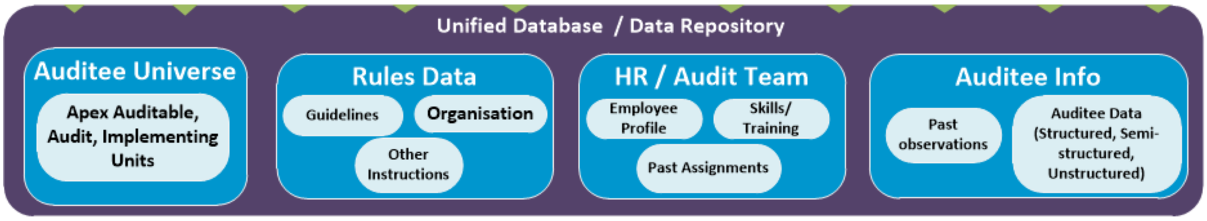
4. Layer 4: **Services**- The service layer consists of services which shall be used by any application



5. Layer 5: **Integration layer**- refers to the integration layer which will act as a bridge between the external and internal Applications. It will expose the services in the architecture in a consistent manner while enabling services to be implemented in a variety of technologies.

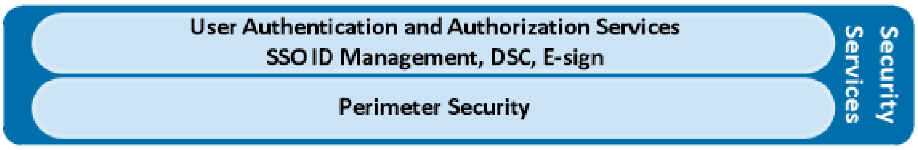


6. Layer 6: **Data layer**- refers to the databases of OIOS Application which will be populated/ referred to by the various applications/ services. It illustrates the idea of enterprise data (not departmental data or departmental extensions to enterprise data) and how it should be logically visible and consolidated by data domain. This does not imply that, all data must be physically located in the same database, or managed by the same system, but that there are coherent set of rules for locating, a unified view of, and a standard way to access the data.



7. Layer 7: **Security services** – the layer, while being conceptually similar to other types of services has been shown separately because it has a significant impact across levels within the

architecture. It shall provide secure access and control to data, services, applications and user interfaces.


User Authentication and Authorization Services
SSO ID Management, DSC, E-sign
Perimeter Security
Security Services

- OIOS is proposed to be integrated software application, deployed centrally at Data Centre (DC), having Web Portal interface.
- The OIOS Application will be a bespoke application, with **configurability** at its core to enable all configurations including policy decisions, operational parameters, rules etc. shall be captured and metadata maintained within OIOS System.
- The system shall provide facility to the decision makers to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace. Detailed examples of configurability have been provided in Vol 1, Annexure A of this document.
- This shall be achieved through the master maintenance of modules and functionalities, wherein the authorized resources will be able to enable, disable or configure the different functionalities, based on Role Based Access Control (RBAC) for individual IA&AD office requirements, but the application shall work on a common architecture, configuration and functional modules.
- Decoupling of business parameters/ workflows/ rules engine/ master data from the rest of solution architecture and making them configurable will allow flexibility.
- The core modular, fully integrated and automated application for the IA&AD users, shall have:
  - Interface for various types of Users and applications
  - It is envisaged that the core application should have **decoupled but integrated core database**, though there may be logical partitioning for effective data retrieval and storage
  - In addition to the above, it is also proposed that the entire application architecture will have a ‘Business Logic layer’ and a ‘Data Access Layer’ to support the efficient data handling between the ‘Application Layer’ and the ‘Database Layer’
  - The OIOS application and its functionalities should be granular and modular enough for the administrators to enable or disable any particular function of OIOS at any IA&AD office, at any given time, as per their requirement, without the need for a developer / code level change / custom UI change.

3. Application Architecture

Principles

1. Ease of Use: Applications are easy to use, with a friendly, intuitive, customised UI for users requiring no specialised IT skills.
2. Sharing & Reusability: All commonly used Applications are abstracted to be built once and deployed across the Organisation through reuse and sharing. Sharing & Reusability shall be subject to conformance with the principles of Security & Privacy.
3. Technology Independence: Application Design is open standards-based and technology-independent.
4. Application Security: Applications are secure by design and developed using secure coding standards and practices.

3.1. Application type

The OIOS Application Type grouping has been done on basis of functionality (as in Section 11 of Vol 1 of this document) and their use across different IA&AD offices and department users. The application types are:

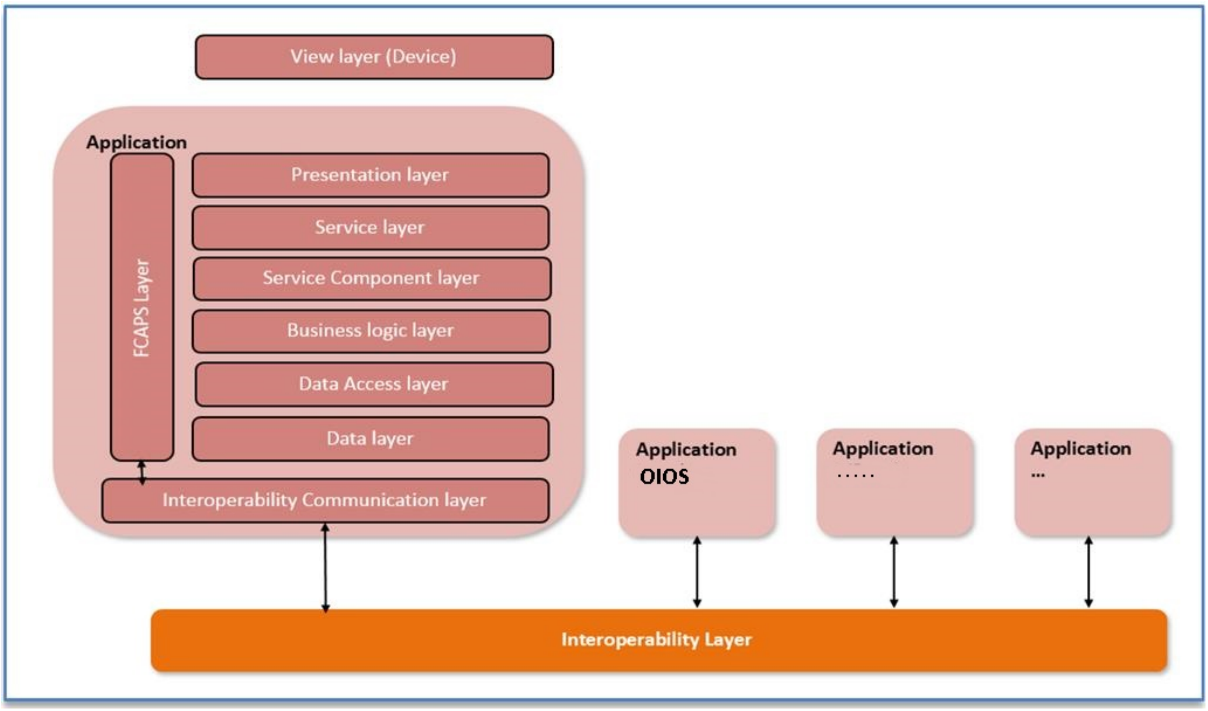
- Audit and related services
- Master Data services
- Common Services

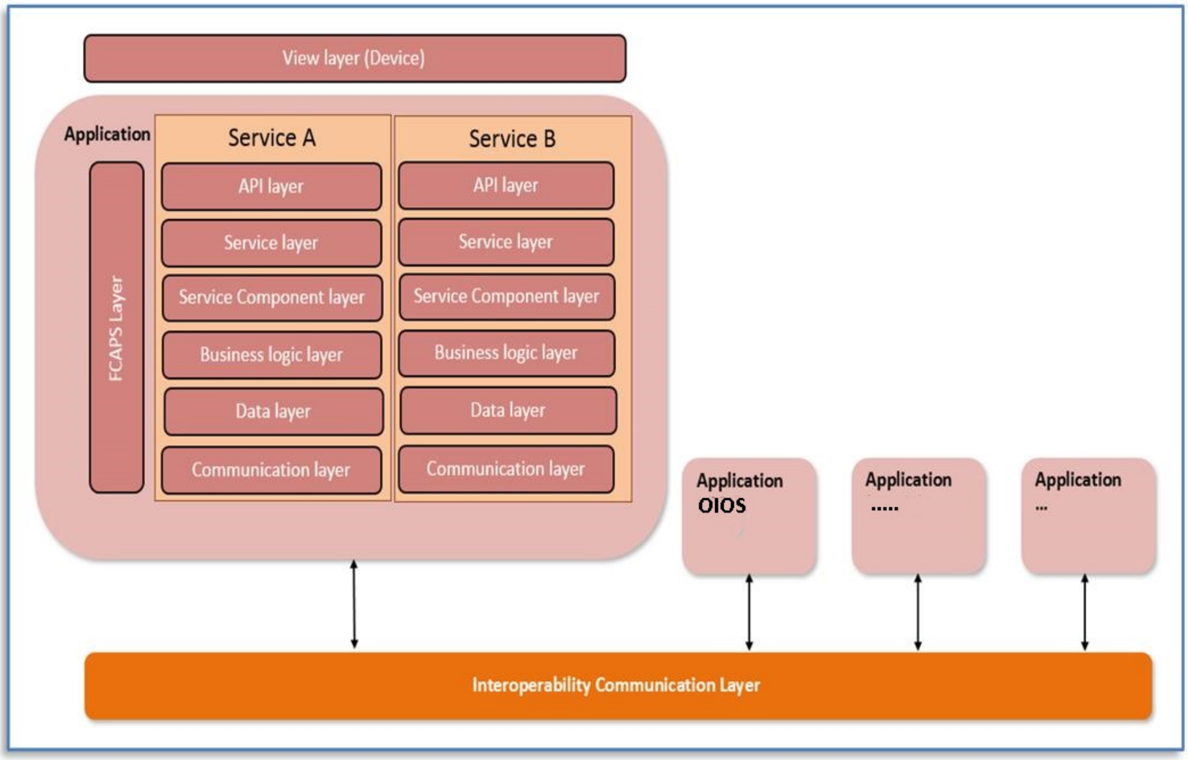
Cross-cutting functionalities of the application shall be designed to deliver a set of related services in an orchestrated manner for multiple field audit offices in response to a single request. All the applications shall inter-operate to the extent needed, mostly through the Open APIs. Annexure A provides details of OIOS modules.

3.2. Application Architecture Meta-Model

This section is added only to provide bidders idea about IA&AD Vision about Enterprise Architecture and is based on IndEA framework.

OIOS Application is envisaged for audit process which shall have multiple solution components, which can be used for subsequent projects. It is therefore envisaged that the IA&AD has a visibility on all its processes and is able to modify them easily with minimum disruption of services. Various services shall invoke multiple applications. The orchestration for each of these services needs to be handled effectively. IA&AD will have a mix of legacy applications (pre-SOA) and SOA compliant applications. The legacy applications shall be taken up later to be made SOA compliant; this is not part of this RFP. In view of the above, Logical Layers of Enterprise Application Architecture are as following: -





View Layer: This layer comprises of thin client, mobile applications, etc. used by the end-user to access the applications.

Presentation Layer: This layer receives inputs from the View Layer and invokes respective services. It is responsible for delivery and formatting of information. It receives the presentation data from application components and returns it to View layer.

Service Layer: This layer comprises of all the Services that are defined in the SOA. The Services can be Individual Service or Composite Service. The Service Layer contains Contracts which binds the Provider and Consumer of the Service.

Component Layer: This layer contains software components, each of which provides the implementation or “realization” for services and their operations. The layer also contains the Functional and Technical Components that facilitate a Service Component to realize one or more services.

Business Logic Layer: This layer enables modelling and designing business processes. A single Service might require interaction of various departments to fulfill the Service. This layer enables mapping the business process and simulating the process. On successful simulation, the process can be deployed in real-time. It also provides for easy change of business processes and its percolation across various departments.

Data Access Layer: This layer provides data from the Data Layer to Business Logic Layer.

Data Layer: This layer comprises of the Applications Database.

Interoperability Communication Layer: All integrations shall be affected through this layer. This layer facilitates effective Mediation Services, provides Adapters, Transport protocols, Service Management, Security features, etc. Translation Logic required for integration is built in this layer.

Application: Applications comprises of both, SOA compliant and legacy applications.

FCAPS Layer: This is the management layer responsible for managing the application component. FCAPS stands for Fault, Configuration, Accounting, Performance and Security functions. This layer supports interface for management applications to effectively and efficiently manage the performance of the application.

3.3. Application Architecture Standards

The envisaged IA&AD’s Enterprise Application Architecture intends to ensure interoperability of all the applications in the system along with seamless upgradation/ migration and addition of new applications to the system. The Enterprise Application Architecture should adhere to applicable standards, such as:

a) **Interoperability Framework for e-Governance (IFEG):**
http://egovstandards.gov.in/sites/default/files/Interoperability%20Framework%20For%20e-Governance%20(IFEG)%20Ver.1.0.pdf

b) **Technical Standards for Interoperability Framework for E-Governance in India**
http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf

3.4. OIOS Architecture Guidelines

3.4.1. Open source software

OIOS application shall prefer open source software (OSS) to closed source software (CSS). OIOS applications must comply by the "Policy on Adoption of Open Source Software for Government of India". For Further details, please refer to:
http://meity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf

3.4.2. Open Application Programming Interfaces (APIs)

The OIOS Application Architecture shall use Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations.

All applications must comply the "Policy on Open Application Programming Interfaces (APIs) for Government of India". For Further details, please refer to:

http://meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf

Specific OEM products may be used when necessary to achieve scale, performance and reliability. Every such OEM component/service/product/framework/Managed Service Provider pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using the same standard/API before it can be used to ensure system is not locked in to single vendor implementation.

3.4.3. Platform Approach

OIOS system will be built as a platform. This means that OIOS system will be built entirely with open APIs, and the system features can be accessed via any user interface (internal or 3rd party applications) that works on top of these APIs.

Openness - Adoption of open API, open standards and wherever prudent open source products are of paramount importance for the system. This will ensure the system to be lightweight, scalable and secure.

Openness comes from use of open standards and creating vendor neutral APIs and interfaces for all components. All the APIs will be stateless. Data access must be always through APIs, no application will access data directly from the storage layer or data access layer. For every internal data access also (access between various modules) there will be APIs and no direct access will be there.

3.4.4. Platform & Database Agnostic

OIOS Application shall be forward compatible. They shall be deployable on any technology platform and shall be able to communicate with any data store.

3.4.5. Application design for occasionally connected systems/ offline functionality

Refer Vol 1, Annexure A for offline functionalities. For the small percentage of functionality that requires “occasionally connected/offline” operations, applications may be designed to use a local persistent store/cache just for the purposes of offline capability and later synchronize with the host application as and when connectivity is restored. As connectivity becomes ubiquitous, less need for such offline capabilities will be felt.

3.4.6. Secure Coding Practices

The OIOS applications must adhere to Standard Secure Coding Practices. For example, while designing and implementing access management, session management, password protection, data protection, Error handling and log management, etc. Indicative standards for Secure Coding are available in **ISO/IEC TS 17961:2013** (Information technology -- Programming languages, their environments and system software interfaces -- C secure coding rules).

3.4.7. Non-Functional Requirements for architecture

1. Reliability

The system must have appropriate measures to ensure processing reliability for the data received or accessed through the solution. It will be necessary that the following issues be taken care properly.

a. Prevent processing of duplicate incoming files / data

b. Zero loss of data (data already saved / data at rest should also not be lost)

c. Unauthorized access and alteration to the Data uploaded in the OIOS system shall be prevented.

2. Ease of Use

Ease of use such that applications are easy to use, with a friendly, intuitive, customised UI for users requiring no specialised IT skills

3. Multiple language Support

OIOS must be able to capture data in various fields in multiple Indian languages. It should facilitate typing in vernacular languages, including the facility for transliteration and also provide for a dictionary (with words being auto-populated as well as user-added) to facilitate multi-language search. Majority of users for Indian languages would use Hindi, so support for *Devanagari* script is the first priority

4. Scalability

The OIOS application should be able to scale elastically to handle the increase or decrease in workload.

The Application must support load balancing and routing.

The Application must support horizontal scaling of Servers, compute, storage, network, etc.

Graceful failure: The application must not have any Single-point of failure. There must be a graceful degradation of services in case of any failure.

5. Performance

The Application must comply by Service Response Time as required by the Application and stipulated in the SLAs.

6. Security

Security solution for OIOS architecture should comply with the specifications as stated in this document and the annexure C of Vol 1 of this RFP.

7. Usability

The applications must comply with ISO 9241-210:2010 Standards (Ergonomics of human-system interaction), GIGW Standards and other standards as stipulated by GoI.

8. Quality

The applications must comply by ISO/IEC 25010:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, GIGW standards and other stipulated standards.

9. Availability

All Applications must support the Availability SLAs as mentioned for each application. The system must meet the stipulated RTOs and RPOs.

10. Recovery

The applications must comply by the Recovery Point Objective and Recovery Time Objective as stipulated in the SLA.

11. Error Handling & Resolution

The applications must efficient error handling. It must also provide detailed logs to enable efficient de-bugging and issue resolution. A repository of 'Known Issues' must be made available to the System Administrator.

12. Documentation

All Software documentation including but not limited to following must be maintained with proper Version Control and Access Rights. Software Traceability Matrix must be maintained:

a) Requirement Gathering, SRS, Gap Analysis, Design, Testing, Use Cases, User Guides, etc.

b) Project backlog, sprint backlog, release backlog, Executable specifications, retrospective document/ templates

13. Support for Differently-Abled Users

All applications must support accessibility by Differently-Abled Users and adhere to GIGW Standards.

14. Change Control

The Product owner must approve and monitor the changes that are done to the software. All Change Request documents must be approved before implementation and Unit Testing.

15. Sharing & Reusability

All commonly used applications are abstracted to be built once and deployed across the Whole-of-Department through reuse and sharing. Sharing & Reusability shall be subject to conformance with the principles of Security & Privacy.

3.5. Miscellaneous

3.5.1. Email service

NIC Email services are envisaged to be used as a part of the solution to send alert/ intimations / automated messages to the registered email ids, based on preferences set up/ opted by individual users.

3.5.2. QR Code

QR codes are envisaged to be part of solution for all the outputs generated from the OIOS system. QR code generation/tagging and printing should be part of the system, whereas QR scanning may be incorporated in proposed mobile application of OIOS.

4. Data Architecture

Data architecture provides a mechanism for the IA&AD users at various levels to identify, discover, describe, manage, protect and share the data, reuse information consistently within and across the IT applications of auditee entities and other government departments.

4.1. Principles

1. Data Asset: Data is an asset that has a specific and measurable value to the department and is managed accordingly.
2. Data-sharing: Data is shared across IA&AD, subject to rights and privileges, so as to prevent creation and maintenance of duplicative sets of data.
3. Data Trustee: Each dataset has a trustee accountable for data quality and security.
4. Data Security: Data Security: Data is protected from unauthorised or unlawful processing, accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, through adoption of international standards and best practices, duly protecting the privacy of personal data and confidentiality of sensitive data .
5. Common Vocabulary and Data Definitions: Data is defined consistently throughout all levels of Government, and the definitions are understandable and available to all users.

4.2. Metadata and Data Archival –

The proposed OIOS solution should support archival of digital documents in any format (like PDF, PDFA, Word, Excel, Image, etc.), support roles and rights-based security where there can be multiple levels of access right to the content like read, create, modify, delete, etc. The proposed solution should support inbuilt "Document Image Viewer" for displaying image document without native viewer.

The proposed solution should support the search functionality within the content. It should support search criteria like search by metadata fields, content objects, documents, pages, etc. It should support Full Text Search on image and electronic documents.

4.3. Data Standardization and Master Data Management

Master Data is critical to ensure that all applications use standard set of data and thus are able to interoperate with one another in a meaningful manner. It should be ensured that users don’t maintain their own list of values or manage a copy of their own.

5. Technical Architecture

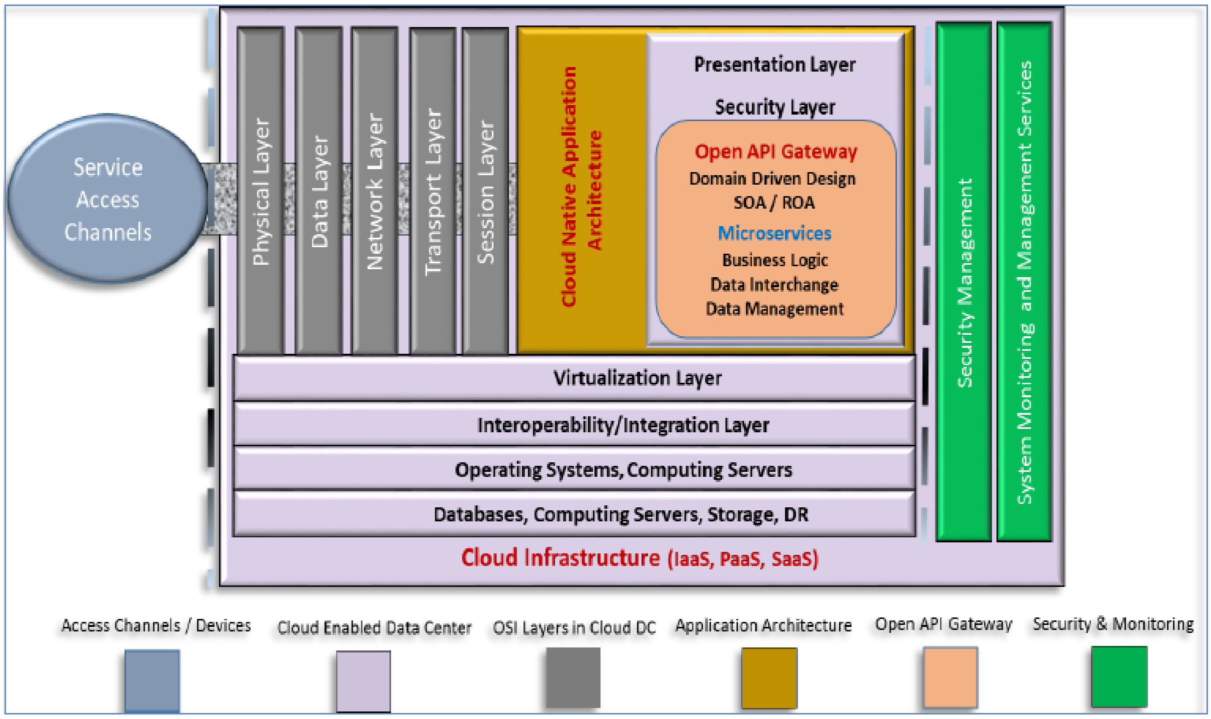
Principles

1. Technology Independent Architecture: need to be developed in a technology-neutral manner so as to avoid captivity to a specific product or implementation method.
2. Future-proof Architecture: OIOS need to be suitably designed and developed so as to be future-proof, not requiring frequent revisions with the advent of every new technology.
3. Open Standards: Open Standards need to be adopted in the design and implementation of OIOS.
4. Shared Infrastructure: IT Infrastructure is shared to ensure optimal utilization and effective maintenance.
5. Mobile: Mobile channel with limited functionality for delivery of all services, among all delivery channels.
6. Availability: The OIOS along with the applications and services are available 24 x 7.

5.1. Open API – Based Architecture

This section is added only to provide bidders idea about IA&AD Vision about open API based Architecture and is based on IndEA framework.

The functional diagram for Virtualization of OIOS Services using Open API Gateway on Cloud is illustrated in the diagram below:



The OIOS system to be designed to expose different sets of distinct APIs for the consumption of G2G services and one for internal use to manage the entire system in terms of hot fixes, deployments, configurations, monitoring and security services. These APIs shall be centrally configurable based on the change in government policies and business rules. The APIs may be RESTful, XML-based, and stateless services wherever micro services are defined, and it should be SOA based for integrated services (non-micro services). This creates two categories of APIs i.e. RESTful and SOA based.

The use of open APIs addresses loose coupling of components allowing independency of each other and having a service provider neutral layer for allowing use of one or more providers and replacement of a system component with another without affecting other parts of the system. The data access must be always through APIs; no application will access data directly from the storage layer or data access layer. For every internal data access also (access between various modules) there will be APIs and no direct access will be there.

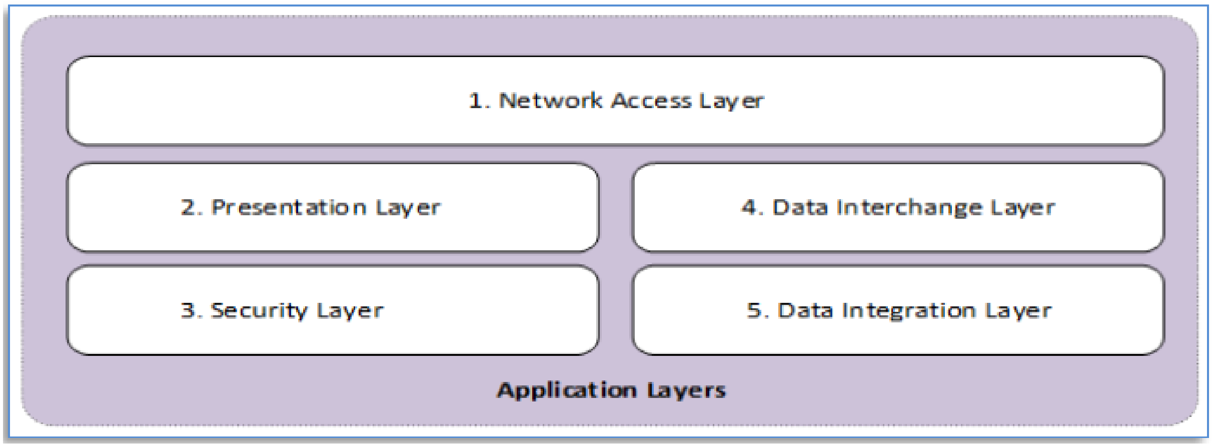
While developing the APIs, it should be ensured that the API end points shall be behind the application's presentation and security layer and it should be consumed via secured VPN (HTTPS protocol) for increased application security. The OAuth 2.0, OpenID and LDAP directory services should be enabled for Open API Gateway to enable application access through secure servers.

As the system will be API driven, the APIs built both by internal and external authorities should go through performance and security measures to increase reliability. For increased security, partitioning, encryption and hashing should be done at the application level and it should not be using proprietary features of the databases used. The security and privacy of data needs to be protected using strong PKI national standards for encryption, use of Hardware Security Module appliances, physical security, access control, network security and through measures such as data partitioning and data encryption wherever applicable.

The containerization of applications has to be done for easy deployment of applications just in time and the container environment variables has to be configured via OS.

5.1.1. Application component standards

The application layer has to support common standards for application level and service level Interoperability. The commonly used Application Layers while designing OIOS solutions is illustrated in the diagram below.



The applicable technology standards for OIOS Application layers are as follows:

Network Access Layer

	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Internet Protocol – 32 bit	IPv4	IANA	1.http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf 2.http://standards.ieee.org/news/2014/ieee_802_11ac_ballo t.html 3. https://tools.ietf.org/html/rfc7540 4. https://tools.ietf.org/search/rfc259 5. https://tools.ietf.org/html/rfc2400
2	Internet Protocol – 128 bit	IPv6	IETF	
3	Authentication and Authorization Data Exchange	SAML 2.0	OASIS	
4	Hypertext Transfer	HTTP/2	IETF, W3C	
5	E-mail Transport	Extended SMTP additions by RFC 5321	IETF	
6	Directory Access	LDAP V3 / X.500-lite	IETF	
7	Domain Name services	DNS	IETF	

Presentation Layer

	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Document type for Simple Hypertext Web Content	ISO/IEC 15445:2000 (HTML 5)	ISO/IEC W3C	1.http://egovstandards.gov.in/sites/default/fil

2	Document type for Complex, Strict Hypertext Web Content (XML or non-XML)	XHTML v5	W3C	es/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf 2. https://www.w3.org/TR/html5/ 3.https://www.w3.org/standards/techs/css#w3c_all 4. https://www.iso.org/standard/66363.html 5. https://www.iso.org/standard/51502.html 6. https://jpeg.org/jpeg2000/
3	Style Sheets (to define Look & Feel of Web-page)	CSS 3	W3C	
4	Extensible Style Sheets (to transform format and addressing parts of documents)	XSL 1.1	W3C	
5	Content for Mobile Devices – Hypertext Markup Language	XHTML Basic v1.1	W3C	
6	Document Type for Editable documents (with formatting)	ISO/IEC 26300-1:2015 (ODF – Open Document v1.2)	ISO/IEC OASIS	
7	Document Type for Presentation	ISO/IEC 26300-1:2015 (ODF – Open Document v1.2)	ISO/IEC OASIS	
8	Document Type for Spreadsheet	ISO/IEC 26300-1:2015 (ODF – Open Document v1.2)	ISO/IEC OASIS	
9	Document type for Non-editable documents	ISO 32000-1:2013 (PDF 1.7)	ISO/IEC	
10	Graphics – Raster Image (Lossy Compression) – Exchange	JPEG2000 /JP2 Part 2	ISO/JPEG Committee	
11	Graphics – Raster Image (Lossy Compression) – Exchange Format for Normal cases (like Web, Desktop applications)	JPEG	ISO/JPEG Committee	

Security Layer

Sr. No.	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Secure Electronic Mail	S/MIME 3.1 / 3.2 latest	IETF	1.http://egovstandards.gov.in/sites/default/files/Technical%

2	Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL	HTTPS	IETF	20Standards%20for%20IFEG%20Ver1.0.pdf 2. https://tools.ietf.org/html/draft-ietf-tls-https-03 3. https://tools.ietf.org/html/draft-ietf-tls-tls13-11 4. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf 5.http://standards.ieee.org/news/2014/ieee_802_11ac_ballo t.html
3	Secure Socket Layer	SSL 3.0	IETF	
4	Transport Layer Security for Server and Web Browser	TLS 1.2 / 1.3 latest	IETF	
5	XML Signature for XML Message signing	XML Signature	W3C	
6	XML Encryption for XML Message encryption	XML Encryption	W3C	

Data Interchange Layer

Sr. No.	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Web Services Description Language	WSDL2.0	W3C	1.http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf 2. https://www.w3.org/TR/soap12/ 3. http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html 4. http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html
2	Web service request delivery	SOAP*1.3*	W3C	
3	Web Services Security - Basic Security Profile	Basic Security Profile V1.1	OASIS	
4	Web Services Security – SOAP message security	SOAP message security *V1.1.1*	OASIS	
5	Web Services Security – Username Token Profile	Username Token Profile *V1.1.1*	OASIS	
6	Web Services Security - X.509 Certificate Token Profile	X.509 Certificate Token Profile *V1.1.1*	OASIS	

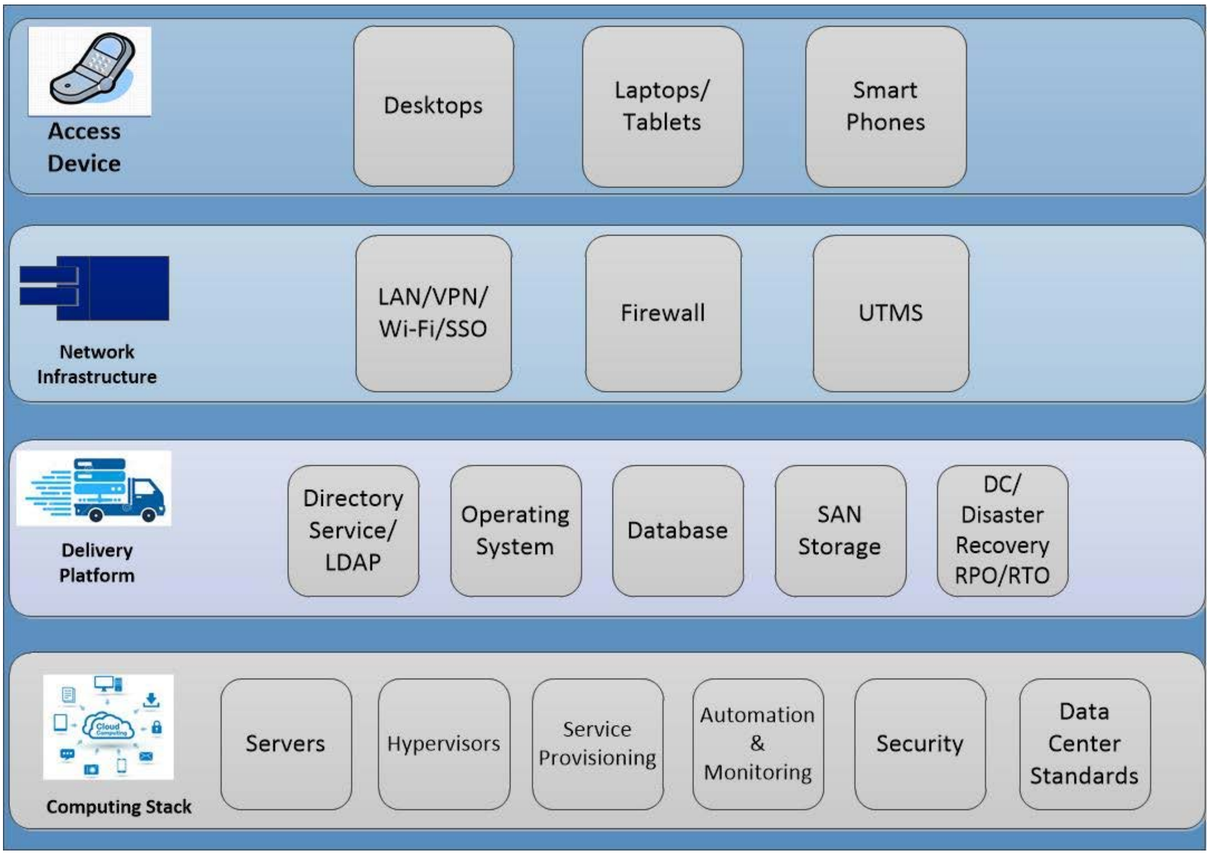
				5. http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html

Data Integration Layer

Sr. No.	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Data Description Language (for exchange of data)	XML 1.0	W3C	1.http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf 2. https://www.w3.org/TR/xmlschema11-1/ 3. https://www.w3.org/TR/xslt-30/ 4. https://www.w3.org/TR/xpath-30/
2	Data Schema Definition	XML Schema (XSD) 1.1 Part 1: Structures, XML Schema Part 2: Datatypes	W3C	
3	Data Transformation for Presentation	XSL 1.1	W3C	
4	Data Transformation for conversion from XML schema format to another format	XSLT 2.0 / 3.0	W3C	
5	Content searching and navigation in an XML document	Xpath 3.0	W3C	
6	XML vocabulary for specifying formatting semantics	XSL 1.1	W3C	
7	Meta-data elements for content	ISO 15836:2009 / 2012 (Dublin Core Metadata Element set)	ISO/IEC	

5.1.2. Infrastructure Component Standards

The infrastructure components required for virtualization of OIOS services and its on-demand delivery using a DC-DR model is categorized into Access Devices, Network Infrastructure, Delivery Platforms, and the Computing Stack. The aforementioned infrastructure components using Open Standards and Formats is indicated in the diagram below:



The open source solution should be used, wherever prudent.

Access devices

Not part of OIOS scope for SI.

Biometric Devices, Smart Cards and Digital Signatures

Not part of OIOS scope for SI. However, the functionality for use of digital signatures for signing OIOS outputs, e.g.: Inspection Report, Audit enquiry etc, must be available.

Network Infrastructure

Sr No.	Service Standards	Description	Open Technology Standards / Specifications
1	**IPv6 / SSO / Directory Services**	IPv6 requires all agencies to transition their equipment and systems that offer or obtain external services to IPv6 standards (from the current IPv4 standards), else the devices / systems that works on IPv6 cannot access /	**1. OAuth** is an open standard for authorization, commonly used as a way for Internet users to authorize websites or applications to access their information on other websites

		render services to stakeholders who uses IPv4 due to address exhaustion. Single Sign On (SSO) enables the user to log in with a single ID and password to gain access to a connected system for seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on directory servers. Directory Services is a network service that discovers and identifies resources on a network and makes them accessible to users and applications. The resources include users, e-mail addresses.	but without giving them the passwords. **2.** **OpenID** is an open standard and decentralized authentication protocol which allows users to be authenticated by co-operating sites or Relying Parties using a third-party service, allowing users to log in to multiple unrelated websites without having to have a separate identity and password for each. **3.** **Lightweight Directory Access Protocol (LDAP)** runs directly over the TCP/IP stack. LDAP is an information model and a protocol for querying and manipulating it. LDAPv3 is an update developed in the Internet Engineering Task Force (IETF) which address the limitations found during deployment of the previous version of LDAP.

Delivery Platform

Sr. No.	Service Standards	Description	Open Technology Standards / Specifications	References for Standards / Specification
1	**SAN Storage**	The storage devices help to save the large amounts of structured and unstructured data, voice and video for future use. The Storage Area Networks (SAN) is the most promising storage technology which helps to access the data at block level to maintain high data recoverability and accessibility.	For SAN: a) FCoE (requires converged network adapter) a. SAN Switch/Director b. IEEE 802.3ae (for 10Gigabit Ethernet over FC) b) iSCSI	NA
2	**Disaster Recovery - RPO / RTO**	The Recovery Point Objective (RPO) i.e. the permissible data disruption time, and the Recovery Time Objective (RTO) is the time taken by the system to be up and running.	RPO should be less than or equal to 15 min and RTO shall be less than or equal to 4 hours.	http://www.digitalindia.gov.in/writereaddata/files/whats_new_doc/RFP%20for%20Accreditatio

				n%2 0of%20Cloud%20Ser vice %20Offerings%20of %20P rivate%20Service%2 0Prov iders.pdf

Specification for RTO/RPO

Specifications
1. The key transaction data shall have RPO of 15 minutes. However, during the change from Primary DC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DRDC and the SI will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements
2. During normal operations, the Primary Data Center (of the Department) will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site
3. In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. Application data and application states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. This is the period during which the Compute environment for the application shall be equivalent to DC.
4. The installed application instance and the database shall be usable and the same SLAs as DC shall be provided. The use of this Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance. The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of Data center. Users of application should be routed seamlessly from DC site to DR site. The SI shall conduct DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss
5. The SI shall clearly define the procedure for announcing DR based on the proposed DR solution. The SI shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The SI shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill g) The SI should offer dashboard to monitor RPO and RTO of each application and database.
6. The SI should offer dashboard to monitor RPO and RTO of each application and database.
7. The SI should offer switchover and switchback of individual applications instead of entire system.
8. Any lag in data replication should be clearly visible in the dashboard and alerts of same should be sent to the respective authorities

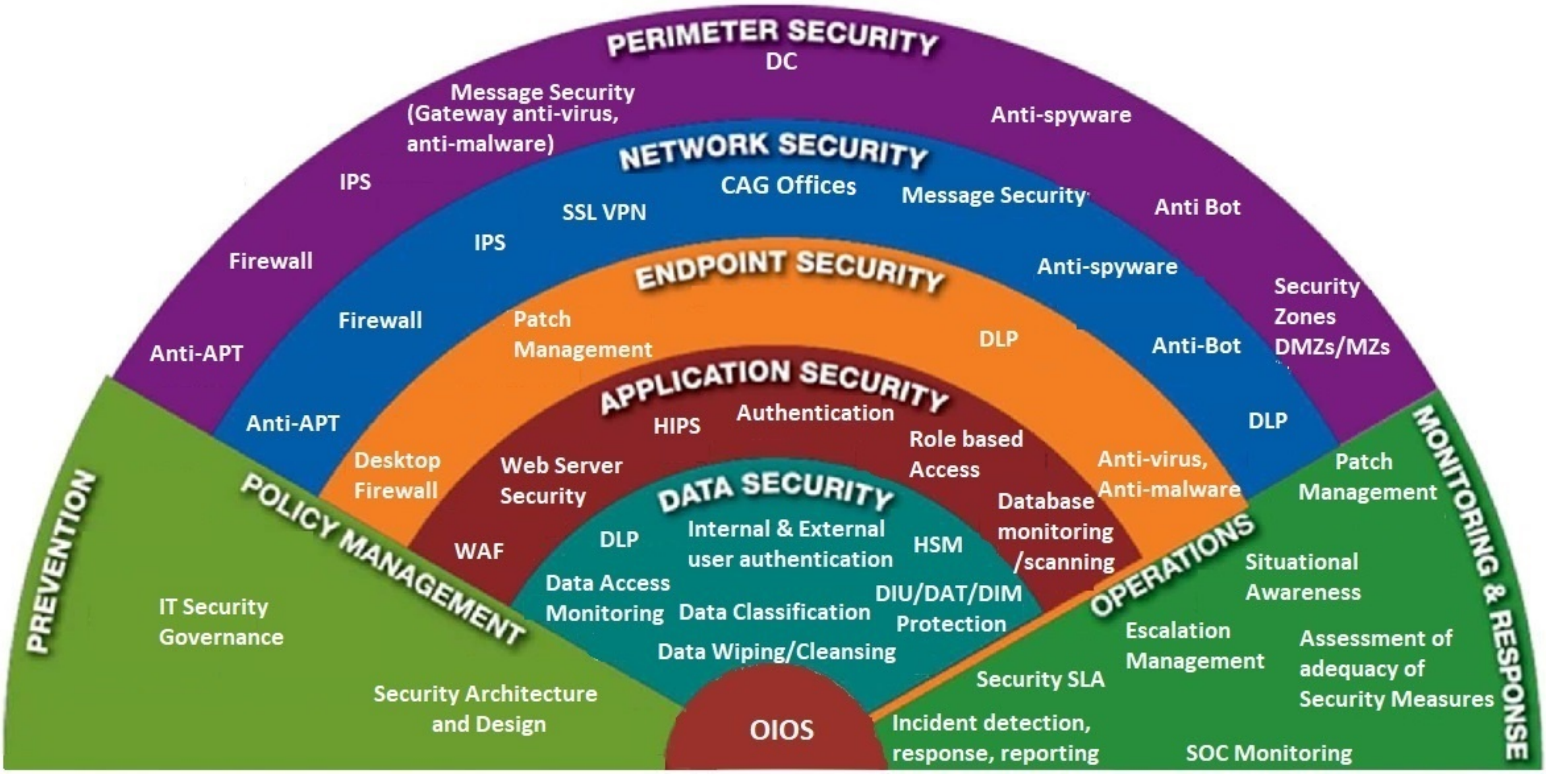
6. Security Architecture

Principles

For designing OIOS Security Architecture, following Principles need to be adhered to:

1. Data Integrity: OIOS Data is correct, consistent and un-tampered.
2. Data Privacy and Confidentiality: Information need to be shared on a Need-To-Know basis and is collected/accessed/ modified only by authorized personnel.
3. Non-repudiability: OIOS should ensure non-repudiability of information in the system.
4. Secure by Design: Security has to be built into all stages and all aspects of architecture development.

6.1. Security Architecture



The envisaged Security architecture for OIOS covers following layers:

a) Perimeter

b) Network

c) End point (PC, laptop)

d) Application

e) Data

In addition, the above need to be supported by following: -

a) Operations

b) Policy management

Based on the Security Architecture, the envisaged security measures for OIOS, are listed in the table below:-

S.N.	Area	Protection measure	Applicable to
1	**Operations: Security monitoring**		
1.1	SOC monitoring	Security operations Center	At IA&AD office
1.2	Security dashboard	Security information and event management (SIEM)	At IA&AD office
1.3	Patch management (Common to all layers)	Prompt installation of patch (es) released by system software OEM	All servers
1.4	Incident detection, response, reporting	Monitoring and analysis	IA&AD with help of SOC Team
1.5	Escalation management	Escalation matrix	IA&AD with help of SOC Team
1.6	Security SLA	Monitoring and reporting	System Integrator, PMT
1.7	Assessment of adequacy of Security measures	Audit	Security audit by STQC/ STQC/ Cert-In empanelled agencies

S.N.	Area	Protection measure	Applicable to
1.8	Situational awareness	Security training	IA&AD
2	**Perimeter Layer**		
2.1	Proactive monitoring of scouting effort by hacker	Anti-APT (Advanced persistent threat) solution	Data Centers
2.2	Perimeter security	a) Firewall b) IPS (Intrusion prevention system) c) Message security: Gateway anti-virus, anti-malware d) Anti-spyware, Anti bot	Data Centers
2.3	Secure DMZs/ MZs	Security zones using Firewall	OIOS Deployment
3	**Network Layer**		
3.1	Proactive monitoring of scouting effort by hacker	Anti-APT (Advanced persistent threat) solution	IA&AD offices
3.2	Network Gateway security	a) Firewall b) IPS (Intrusion prevention system) c) Message security: Gateway anti-virus, anti-malware Anti-spyware, Anti bot	IA&AD offices: HQs, Field audit offices
3.1	Data loss prevention	Network DLP	IA&AD offices gateway
3.2	Data in transit	SSL VPN	Application based, network based

S.N.	Area	Protection measure	Applicable to
4	**End point Layer (Not in SI's scope of work)**		
4.1	Desktop firewall	OS personal firewall	Office computing devices: PC, Laptop
4.2	Patch management: OS, software	Regular updates	All Office computing devices
4.3	Data leakage prevention	DLP	Standalone PC handling sensitive information
4.4	Anti-virus, anti-malware	Anti-virus	All Office computing devices
5	**Application Layer**		
5.1	Separate Application Firewall	Web Application Firewall	MZ of DCs
5.2	Web server security	URL filtering, Caching at Gateway	DMZ of DCs
5.3	Application server	HIPS	MZ of DCs
5.4	Authentication	Using SSO in conjunction with IDAM	All Applications
5.5	Role based access	Using LDAP, Application, Database controls	OIOS
6	**Data Layer**		
6.1	Database Server	DLP, HIPS (Host based Intrusion prevention system)	MZ of DCs
6.2	Data access monitoring	Privilege access management, Database Activity monitoring	Database server, other servers

S.N.	Area	Protection measure	Applicable to
6.3	Id & Access Management: Internal User Authentication	SSO: Implementation of Open source LDAP Directory Service Assigning Role based privileges 2 factor authentication	IA&AD staff
6.4	External User Authentication	2 Factor authentication	User name, password/OTP
6.5	Data in use/ storage	Encryption	Encryption of field (s)
6.6	Data at rest	Database Tables at Operating system in encrypted form	RDBMs
6.7	Data in motion	Encrypted pipe for database to database data exchange	(Database level)
6.8	Data wiping/ cleansing	Feasible only at PC, Laptop	Unserviceable hard disk to be destroyed
6.9	Storage of Security encryption keys	Hardware Security Module	Encrypted data of Aadhar number stored in database
6.10	Data classification	Secret/ Top secret data (as per GoI data classification norms) not to be stored in Database	IA&AD users
7	**Policy management (Not in SI's scope of work)**		
7.1	IT Security Governance		IA&AD
7.2	Security Architecture & design	OIOS, Other Projects	IA&AD

Functionality at different layers is provided in subsequent sections.

6.2. Security Functionality – Perimeter layer

The main functionalities at the Perimeter layer are to identify the appropriate security for every asset, application / service and data. The access to various assets, the appropriate configurations at various levels should be done at this layer.

a) Secure DMZ/ MZ – Design the DC network considering the sensitivity zones.
b) IPS – Intrusion prevention at physical layer
c) Firewalls – to protect the infrastructure from unwanted or black listed intruders.
d) Content Filtering - Screen and exclude from access or availability, Web pages or e-mail that are deemed objectionable.
e) Message Security (anti-virus, anti-malware) – Appropriate anti-virus and anti-malwares should be identified and deployed. Policy regarding the same should be made to inform all the concerned.
f) Data Loss Prevention
g) Buffer Overflow Exploit Protection

6.3. Security Functionality – Application layer

The functionalities mentioned below should be provided at the OIOS application layer to secure the service / application and its data:

a) Static testing and code review - Purpose of this type of testing is to identify the vulnerabilities without carrying out the actual execution of the code. Development or implementation team does this testing and provides the reports related to the same.
b) Dynamic application testing- Purpose of dynamic application testing is to determine the associated security vulnerabilities in the code by executing it. This helps to identify the security issues related to the complete production set-up including the exact version of the application and application stack.
c) Web application firewall: Firewalls at application level should be given consideration to prevent attacks such as SQL injection, Cross Site Scripting (XSS), cross site request forgery etc.

d) Vulnerability assessment and penetration testing: Objective of carrying out the VAPT is an identification of vulnerabilities and possibilities of their exploitation.

e) User Authentication: There should be a proper authentication mechanism being implemented in the applications for providing an access to the sensitive information to the users.

f) Database monitoring- Monitoring the application, database servers for their uptime, threats which are being observed

g) Role/ Rule based access: A proper authorization policy and rules should be defined to prevent the unauthorized access to the various areas of the application.

6.3.1. API Security

It is possible to attack or leak data in transit while calling the API and hence the API design is equally crucial when talking about security. The following care must be taken while designing API:

a) Information required for routing or interpreting the contents of the packet should be part of header and should be appropriately tagged.

b) The body of the packet should be encrypted and should not be easily accessible. User's personal identity information should be part of the body of the packet and not the header.

c) Provide some default value for optional parameters/ tags.

d) Only necessary information should be taken from the user and unnecessary information exchange should be avoided.

e) Preferably no personal information should be shared as a part of response.

f) API should be made available only on the secured channel.

g) Access to API should be provided only to the authorized users.

h) Whenever data is exchanged between two servers, it should be done only after proper white-listing of the IPs; requests should not accepted from any other IPs.

i) Mobile apps - Sensitive or personally identifiable information should not be shared through such apps as the authenticity of the end user is questionable and also because mobile apps can be easily reverse engineered to retrieve the tokens etc. which are used to communicate with the server.

Aadhaar APIs can be considered as a reference for designing secured APIs (Ref. https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf).

6.4. Security Functionality – Data layer

Below functionalities should be provided for data layer:

a) Data needs to be secured when at rest, at motion i.e. in transit or in use – Every piece of data irrespective of its sensitiveness need to be secured against the threats of unauthorized access, data corruption or complete data loss Depending on the sensitivity and availability needs, methods should be applied to secure the data.

b) Identity and access management for data – The data should be accessible to only authorized persons, at appropriate time and only for the specified purpose.

c) Access Right Management – Access to data should be restricted by creating and applying a policy for every kind of data set. Data access policy will define the constraint for controlling the data access by its users. It will help in applying appropriate read, write controls over data elements.

d) Data Integrity monitoring – Data Integrity is as important as any other aspect of data security. If the correctness of data cannot be determined, it is almost same as data loss. In some cases having data with compromised integrity is more dangerous than having no data. Therefore mechanism needs to be applied to monitoring data integrity at various stages to enhance authenticity, reliability and availability of data.

Comptroller and Auditor General of India

Selection of System Integrator for Implementation, Roll Out and Operations & Maintenance of

‘One IA&AD One System’ (OIOS) Project

VOLUME – I – Annexure C

Page Intentionally Left Blank

Contents

1. Overview

This document details the IT Infrastructure and Security solution requirements for the OIOS Application. All items in this document (except where mentioned otherwise) are deliverables to IA&AD by the SI. The definitions as they appear can be referred from RFP Volumes.

1.1. Design Considerations:

The OIOS shall be built following the design considerations as given below:

1. **Ecosystem and API based Approach:**

   Stakeholders (internal as well as outside IAAD) would interface with OIOS via OIOS web application or via ecosystem supported applications with limited functionalities such as Data Analytics application, Audit response application. The external stakeholders would process the information in their respective systems and re-transmit the processed information to the OIOS - which would be available for internal stakeholders for viewing/ processing and generating various MIS reports. The external users/platforms may have limited access to OIOS Application through temporary sign-on credentials/ APIs. One of the design considerations for OIOS is to provide such interfaces to OIOS Application for the stakeholders/ external applications.

2. **Provision of a Scalable Solution**

   The OIOS solution is expected to be functional for at least 10 years after phase – II deployment. The solution would be done keeping in mind the scalability (storage and processing power) of the system. All India roll out of the OIOS application (in phase-wise manner) and annual periodicity of the audit processes is expected to lead to huge growth in the database. Every component of the OIOS System needs to be scale horizontally to large volumes of data.

3. **Distributed Access:**

   The IAAD field offices are distributed across India and field office parties would not be necessarily be stationed at the IAAD field offices. Considering this, an offline application with limited functionalities is included in the OIOS design to provide access to field audit parties.

4. **Security and Privacy:**

   In addition to the restricted-access audit product being processed and finalized in the system and personnel information of IAAD employees, the OIOS is designed to access and store data from other governmental departments/ third party organizations. Security and privacy of data should be fundamental in design of the system without sacrificing utility and user-friendliness of the system. When creating a system of this scale, it is imperative that handling of the sensitivity and criticality of data are not afterthoughts, but designed into the strategy of the system from day-one. The system should comply with the benchmarks for confidentiality, integrity, availability and non-repudiation of information stored/generated by the OIOS Application.

5. **Configurability of Business Rule Driven Approach:**

   The Audit process (Document management system) would differ significantly across streams of audit (Civil, Railways, Defence etc.), types of audit (compliance, financial, performance) and to some extent various offices (Civil Audit offices in Allahabad and Bengaluru etc.). The OIOS is designed to include configurability of business rules including policy decisions, business parameters etc. place within the system.

   The system shall provide facility to the decision makers to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace. Managing these in a central repository ensures only once source of truth is used across many application servers and reduces issues of inconsistent application behavior. Decoupling of the business parameters/rules/master data from the rest of the solution architecture and making them configurable allows for a great deal of flexibility. There should be a central interface for managing the configurability by authorized user group.

6. **SLA driven solution**

   An Enterprise Monitoring System (EMS) is included in the OIOS solution to provide for single platform for the data to be readily available (real-time), aggregated, classified and stored, so as not to delay the business processes of monitoring and decision making. The solution should include the facilities for timely access of analytics reports at every level and department of the organization and provide timely analysis of data as well as monitoring of KPIs through SLAs, resulting in effective service delivery and improved decision making.

2. OIOS System IT Infrastructure Requirements

1. The proposed solution of SI should meet the minimum specification requirements for respective component, bidder needs to size the solution components to meet the project requirement. In case any of the systems / appliances could not meet the performance requirement during the implementation testing or operations phase, SI will be responsible to change the same with equivalent/better product without any additional cost to IA&AD.
2. All components to be maintained in redundancy based on the SLA requirements, architecture and performance. Bidder needs to provide the compliance with respect to each clause and clear reference-able document, highlighting how the stated requirement is being met. All components should be sized to meet the required performance and SLA level when one of the redundant devices is down.
3. The proposed solution should be optimized including bandwidth (within the scope of SI) while ensuring high availability and no single point of failure across the architecture.
4. The proposed systems should be of enterprise class and must be current as per OEMs latest offering, in line with advancements of technology in these domains. Bidder needs to provide the published benchmarks for the stated systems along with the sizing assessment sheet being certified by the OEM/ SI (as applicable) for the stated systems. All the components should be able to handle expected loads and provision the desired transaction times and throughputs.
5. It is to be noted that bidder needs to provide a detailed assessment sheet taking into considerations the volumetric and other details given in the RFP. The assessment should clearly highlight the sizing parameters taken into consideration while designing the solution and also should be provided on OEM / SI letter head, along with publicly available published benchmarks. Detailed worksheets of transactions assumed per second, CPU or Core-wise need to be shown, scaled upwards to handle the desired volumes and traffic along with the desired scalability.
6. The database layer should utilize the database servers for consolidating the database requirements. The architecture should have horizontal scalability. Benefits/additional security, reliability, availability features at the server level architecture would be given due consideration during evaluation.

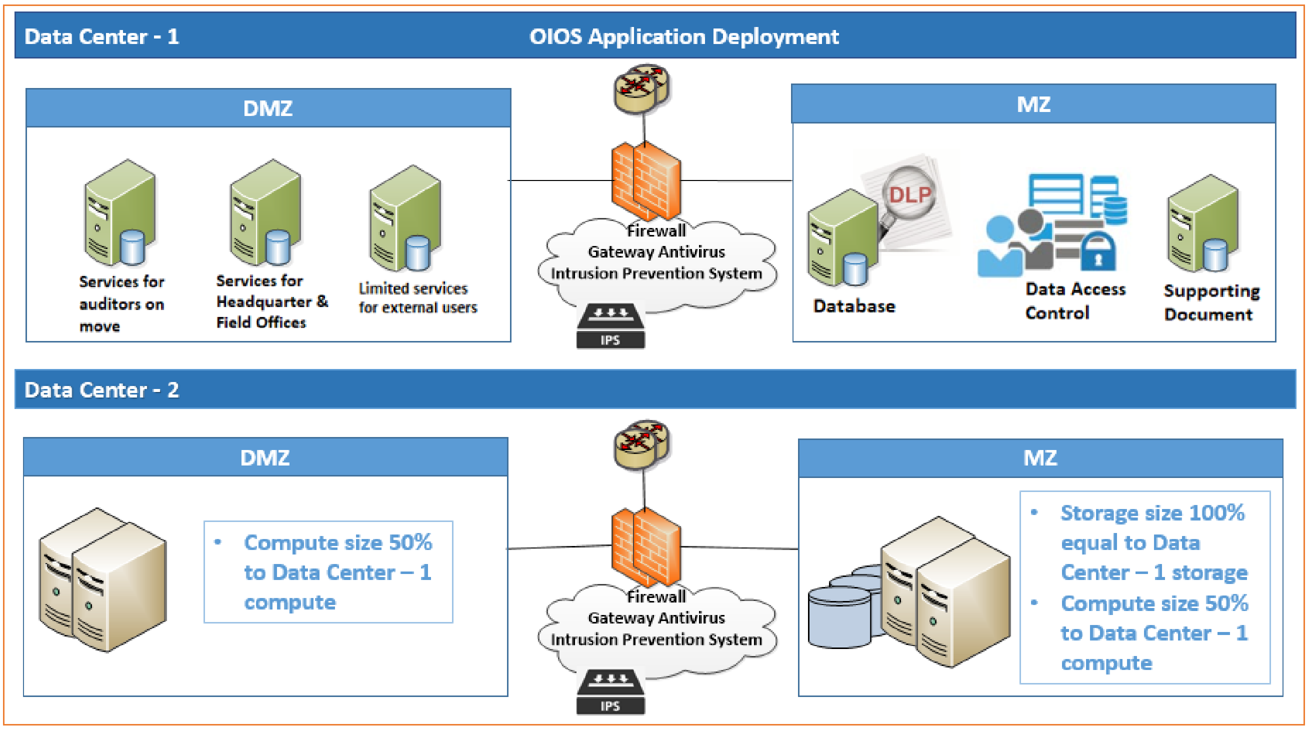
7. The systems architecture should clearly demonstrate and highlight the key requirements of IA&AD viz reliability, availability, scalability, survivability, resilience and serviceability of individual critical components as well as the OIOS system as a whole.
8. SI needs to comply with the availability requirements as stated in the SLA (Annexure to Volume-3 for RFP) for the OIOS system as a whole. This availability is to be measured on a monthly basis.
9. Redundancies/teaming should be maintained at different interconnecting fabrics so as to avoid any single point of failure / performance bottleneck.
10. Networking equipment should be capable of processing IPv4 & IPv6 traffic. Security features that are delivered shall be IPv6 ready. All devices should be IPv4 and IPv6 ready from day-1. The proposed solution and all appliances should meet this requirement. The SI shall also be responsible for security adherence on both IPv4 and IPv6.
11. Bidder should utilize virtualization technology to optimize the solution and provide benefits for the overall Cost of ownership and ease of maintenance.
12. Patch management: SI must ensure that all Patches are applied promptly and reports in this regard is submitted periodically.
13. DNS server is required for domain name of DC and the interoperation between Primary DC and Secondary DC (DR) should be such that due to any failure of any/all module at DC level can automatically (manual optional) be operated from Secondary DC (DR).
14. The Primary DC and Secondary (Disaster Recovery) DC should be architected in such a way that any of the modules may be run from any these data centers, without any impact on the SLAs being defined. The solution should be designed to utilize both the Primary and Secondary Data Centers, so as to enhance security, serviceability and performance. Both the Primary and Secondary Data Centre to be linked to Nearline Data Centre sites.
15. The IT infrastructure (as stated in the subsequent sections in this Report) proposed for OIOS would comply with the Magic Quadrant listed in latest Gartner report.
    - Bidder should consider the latest Gartner report published on or before last date of bid submission. Any Gartner reports published after that should not be considered.
    - Bidder need to submit a copy of relevant section of the Gartner report along with technical proposal.

- Wherever the Gartner report is not published for any category of the product / solution, the bidder may submit an alternative reputed product analysis report viz Forrester, IDC.
- The COTS products related to IT infrastructure must be from vendors in latest report of the Gartner's Magic quadrant as per criteria defined below:
    a. The OEMs must be in Gartner's Leaders/ Challengers/ Visionaries quadrants. The preference would be awarded in this category as - Leaders (highest)/ Challengers/ Visionaries (lowest).
    b. The product category should have support in India

Note: All the provisions of this Annexure need to be read in conjunction with the provisions of Security and other requirements as mentioned in Annexure-B and need to comply to the same.

3. OIOS System IT infrastructure deployment plan

SI needs to propose the OIOS IT infrastructure deployment architecture to meet the required security guidelines and SLA as per the RFP. Illustrative deployment architecture with minimum infrastructure and security requirements is given below, however SI needs to provide the detailed proposed solution design to meet the requirement of RFP. Detailed requirement related to infrastructure and security as illustrated in the design below is detailed in subsequent sections.


Data Center - 1
OIOS Application Deployment
DMZ
Services for auditors on move
Services for Headquarter & Field Offices
Limited services for external users
Firewall
Gateway Antivirus
Intrusion Prevention System
IPS
MZ
DLP
Database
Data Access Control
Supporting Document
Data Center - 2
DMZ
Compute size 50% to Data Center – 1 compute
Firewall
Gateway Antivirus
Intrusion Prevention System
IPS
MZ
Storage size 100% equal to Data Center – 1 storage
Compute size 50% to Data Center – 1 compute

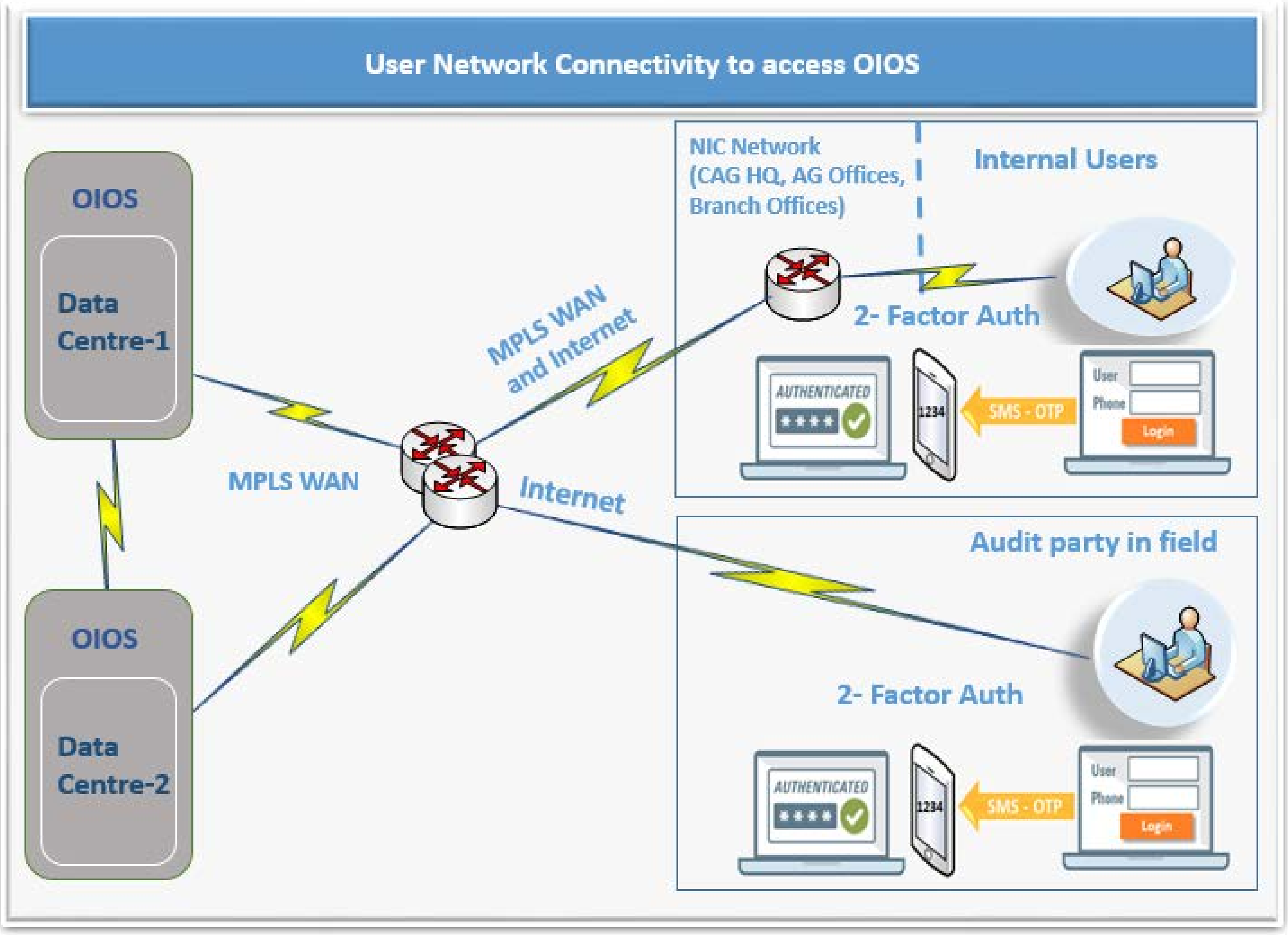
3.1. OIOS Network Infrastructure Requirements

All the material/platforms/software deployed for OIOS application should be enterprise class, to handle expected loads and provision the desired transaction times and throughputs.

The network architecture for user-connectivity to the OIOS Application is given below. OIOS Application shall be deployed on DC DR model. The SI has to setup following environment at DC –

a. Development, b. Testing, c. Training, d. Pre-production and e. Production.

Note: Considering the strict timelines of OIOS Project, it is planned that the Development Environment for OIOS may be setup at SI's proposed cloud/ equivalent model for first three months or till the time SI sets-up DC/DR, whichever is later. The engagement of Cloud Service Provider by SI for initial Development Phase is an adhoc measure. The entire OIOS Application shall shift to DC-1 within 3 months of signing the agreement.



Users shall access OIOS Application as following:

- IA&AD staff at IA&AD offices (HQ, AG office, Branch Office, DG/ PD office) would connect to Data Center through NIC gateway (NIC Net). The connection between the field offices to NIC gateway is via dedicated lease lines and is outside the scope of SI.
- Audit party (users) in field would connect to Data Center using Mobile data internet or NIC gateway (in certain cases).
- The OIOS Apllication would be accessible to the all users through minimum security level of 2-factor authentication.

NOTE: IAAD may decide to exercise the option of engaging VPN Services for mobile users as an added security requirement. The timeline for VPN implementation shall be decided by IA&AD as and when required.

4. OIOS Security Requirements

OIOS Hosting architecture shall have standard Demilitarized Zone (DMZ) and Militarized Zone (MZ). The application components shall be deployed in two zones as following:

- DMZ : Front-end applications – field users' access to OIOS applications.
- MZ : Back-end applications – Database administrator's access to OIOS Core Application, Database and supporting document. This needs higher security.

The solution of SI needs to ensure Confidentiality, Integrity and Availability of all information and data repositories of OIOS through its solution as per the SLAs and the requirements stated in this RFP. The security requirement for OIOS at various layers is given in Annexure B of RFP Volume – I, as read in conjunction with this Document.

This document provides additional details of security infrastructure requirements. SI shall propose the infrastructure security architecture of OIOS to ensure the required security level for OIOS data center infrastructure. Key requirements of infrastructure security are:

a. **Security Standards:** The SI shall propose the security solution based on the compliance to following standards:

   - ISO 27001:2013 Certification
   - ISO 27002:2013 for implementation of related Code of practice for Information Security controls to be referenced for ISO 27001: 2013 certification.
   - ISO 22301 for Business Continuity Management System.

b. **Perimeter security:** SI shall propose the data center (s) perimeter security to mitigate with various security risks including, but not limited to intrusion prevention, Malware detection/prevention, DoS/DDoS attacks etc. SI needs to ensure that the proposed solution should meet the perimeter security requirements. The proposed solution should include the following components as minimum requirement; however, SI may propose additional components in the solution.

   - **Primary and Secondary Data Centers:**

     i. Firewall: Filter-out the unwanted traffic

ii. IPS: Intrusion prevention in the Data Center from outside network traffic

iii. DDoS Solution: Mitigates risk involving DoS and DDoS attacks

iv. Anti-APT: Static and Dynamic Malware Analysis

v. Web Security Gateway: Filter ingress traffic content

vi. Web Application Firewall: Filter out unwanted traffic of Web Application

- **Primary and Secondary Near Sites DC/DR sites:**

i. Next Generation Firewall: Filter-out the unwanted traffic

c. <u>Data Security and user authentication over Internet link:</u> The OIOS application would engage 2- Factor Authentication mechanism for all field users (except Database administrator, where the security requirements may be stricter). The OIOS application should be compatible to deploying End to End to Encryption across the network (Including IPsec VPN, SSL solutions), if IAAD decides to engage it on a later date.

d. **<u>Security monitoring -</u>** SI needs to ensure the compliance to the security requirement and monitoring of the threats/logs generated by various appliances. The SI shall be responsible for meeting OIOS' comprehensive security requirements and 24*7*365 monitoring, analysis and management to ensure adequate security posture & security compliances. However, IAAD reserves the right to further appoint an external agency to run Security Operation Center (SOC) for monitoring the adherence to security compliance requirements by SI. SOC in that case shall use security tools deployed by SI (at no cost to IAAD) as part of the RFP. The SOC will monitor the security compliance and logs generated by various appliances on behalf of IAAD to provide the compliance report. Engagement of any external agency by IAAD is without prejudice to the responsibilities of the SI as per the RFP.

The below section describes the minimum-security requirements, which has to be complied by the SI during the design, development, implementation and operations phase of the OIOS. The required hardware, software and supporting infrastructure needed to meet the requirements to be included as part of the overall solution.

A.	Information Security Management System (ISMS) – ISO 27001 Certification
1	SI must ensure that the information security management system should be designed, established and implemented for the application and supporting infrastructure based on ISO 27001:2013 standards and ISO 27002 Code of Practices for Information Security controls to be referenced for ISO 27001: 2013 certification The activities to be carried out are as follows: a. SI shall prepare information security policy and supporting processes, procedures and work instructions for ISO 27001 certification and should also integrate with the OIOS information security policy and procedures. The policy and procedure should be submitted within 6 months of the contract signing. b. SI shall carry out Risk Assessment and Risk management Plan for the application and infrastructure, which should include an Enterprise Risk Register as a deliverable with the assessment and classification of all information assets of OIOS. The risk assessment and risk mitigation plan need to be updated on quarterly basis during implementation phase and on quarterly basis during operations phase. c. SI shall make all preparations (activities, documents, etc.) required for ISO 27001:2013 certifications of OIOS. d. SI shall prepare the following policies for OIOS: i. Information security policy ii. Infrastructure and safety policy iii. Third party security policy for users e. SI shall implement all the controls as identified during the Risk assessment and treatment plan as per the agreed timelines. f. SI must ensure that ISO 27001 gets implemented at all the data centers i.e. Primary and Secondary DCs and NLDRs, development environment, staging area etc. and also get the same certified using the ISO 27002:2013 code of practice.

A.	Information Security Management System (ISMS) – ISO 27001 Certification
	g. SI must ensure that the security policies and procedures should be aligned with the Govt of India Regulatory requirements, the IAAD policy and also comply with CERT - IN guidelines/advisories as issued from time to time. h. SI will ensure ISO 27001 half yearly surveillance audits are conducted by the external agency during project duration after Go Live till the contract period. i. SI will ensure that all the observations highlighted during the audit are tracked to closure in specified time frames to be mutually agreed between IAAD and SI. j. IAAD shall appoint a third-party agency for information security audit. It is the responsibility of SI to support and coordinate with TPA and provide the required information for successful audit on a half-yearly basis. Payments to this agency shall be done by IAAD. SI shall ensure that the product / solution required to implement the controls as defined in the ISO 27001standard shall be provisioned / deployed as part of the overall design.
B	**Background Verification:**
1	All key personnel deployed by or on behalf of SI for OIOS project will undergo background check before their deployment. The background verification shall be conducted by SI or an authentic third party.
2	Access controls: SI must ensure that the access rights of all employees, contractors and third-party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change. SI will deploy process and technical control to implement the same.
3	All the resources deployed on the project will sign NDA with SI. SI would certify to IAAD on quarterly basis that all personnel/resources deployed in the OIOS project by SI or any other sub-contractor(s) on behalf of SI have signed the NDA with SI.
C	**Communications and operations management**

A.	Information Security Management System (ISMS) – ISO 27001 Certification
1.	SI shall ensure that all the interfaces between various applications and users are encrypted using appropriate protocols (such as HTTPS, IPsec etc.), algorithm and key management systems. The application and infrastructure should support all the available algorithms. Such facility shall provide support for the following functionality, at a minimum: a) Confidentiality of communication - Encryption of all messages between client and server. b) Authenticity - Authenticate all messages between client and server, confirming the identities of messages/transactions. c) Integrity - Message Authentication Codes (MACs) provide integrity protection that allows recognizing any manipulation of exchanged messages. d) Secure communication between the user and the portal with SSL and encrypted logon information using algorithms with strong key lengths. e) Authorization: Role based access control to authenticated users. f) Non- repudiation: Mechanism to ensure the non-repudiation of authentication
2.	SI will ensure that all the changes made to all assets and infrastructure of OIOS are recorded and logged, stored for at least 12 months, as per best practices and ITIL standards. SI shall deploy Service Knowledge Management System (SKMS) to include all its constituents e.g. configuration management database. The updates to all systems / sub systems / applications and parameters should be approved by IAAD.
3	SI will deploy solution to collate all the logs and maintain a log of all the changes made in the application with date-wise, fortnightly, monthly, quarterly and yearly. Logs shall be available for last 12 months.
4	SI will maintain separate environment for production, test and development to reduce the risks of unauthorized access or changes. No access to production systems / zone shall be permitted from Test and Development zone. No developers / developing team shall have

A.	Information Security Management System (ISMS) – ISO 27001 Certification
	access to production systems. No single DBA should be able to unilaterally make updates to tables / structures / rules / policies.
5	SI will provide for VPN solution for the field users so that applications and functionality as identified can be access from remote location. The solution and type of functionality and module on VPN will be prepared by SI and approved by IAAD at a later date, if required.
6	The systems, sub systems, databases and applications in OIOS should have the functionality to record all the administrator, user level activities including the failed attempts. All types of logging (audit, session, transaction, error logs, diagnostic logging) shall be enabled for databases. SI should size his compute and storage accordingly. The activities to be logged will be approved by IAAD. Ownership and access to log server shall be exclusive from the system owners and should be clearly demonstrated by SI in the Segregation of Duties matrix.
7	SI shall protect logging facilities and log information against tampering and unauthorized access. Ownership and access to log server shall be exclusive from the system owners and should be clearly demonstrated by SI in the Segregation of Duties matrix.
D	**Access Control**
1	SI will create single profile /user database which will act as a master source to provide/ further delegate role-based access to the users.
2	The profile/user database will be managed by respective field offices (Office administrator)
3	Users will be provided single sign ON/off (SSO) functionality to all the applications and modules deployed by SI.
4	The solution should support multiple authentication methods such as Username password, 2-factor authentication, digital certificate *etc.*

A.	Information Security Management System (ISMS) – ISO 27001 Certification
5	Solution should have the capability to define access based on time of day, day of week or by group or user defined access.
7	The solution should have the functionality to provide authentication based on the role/privilege. The solution should have the capability to delegate the role privilege, if required.
8	• The users would have only official (personal name based) email ID (login ID) based access to the OIOS Application. Single/multiple roles may be assigned to one user at the same time (e.g. additional charge of the post). • The Application should allow the user to switch/ toggle across roles. • The DMS Application should be able to demonstrate (provide an audit trail of) the details of user and user roles at the time of activity.
9	• The user authentication to the OIOS application would be based on 2- Factor (password and SMS to the registered mobile number). Any change in the user login credentials would be carried out in NIC servers (outside OIOS Application). However, the OIOS Application should be able to authenticate the login credentials with the NIC database in real-time. • An offline application with limited functionalities is included in this RFP which may be driven by local (to OIOS Application) user credentials. The OIOS solution should be able to deploy and configure password policy as approved by the IAAD in such scenario.
10	All the user activities should be recorded in the system. The system should provide the feature to configure the logs as and when required.
11	The application shall limit more than one session per user. The solution should have the option of blocking multiple sessions for the user.
12	The application should support role-based access control to enforce separation of duties.

A.	Information Security Management System (ISMS) – ISO 27001 Certification
13	The application should display the last login status (successful/unsuccessful time) to the user.
14	The application should not store authentication credentials on client computers after a session terminates.
15	Administrator access - a. SI shall also deploy solution to manage administrator access to the components deployed such as operating system, network, database etc. b. SI shall ensure that direct access to servers / operating systems/ data bases is barred. c. Access to OS / middleware / sub- systems must be through a common access tool that logs all administrator activities The logs should be text-searchable based on key words entered in text.
16	The solution should be compliant with Indian IT Act, 2000 and amendments thereof
17	Logs. All logs of access to systems / sub-systems / applications must be kept for at least 12 months. These logs shall be made available for forensics / fraud investigations whenever required.
18	SI shall ensure that the MIS reports generated from the system shall contain the name of the person generating the report along with date and timestamp in form of watermark.
E	**Information systems acquisition, development and maintenance**
1.	SI will prepare the detail technical security requirement to be submitted to IAAD for review.
2.	SI will define the secure coding guidelines and the same will be approved by the IAAD.
3.	SI shall incorporate validation checks into applications to detect any corruption of information through processing errors or deliberate acts.

A.	Information Security Management System (ISMS) – ISO 27001 Certification
4.	SI shall validate the data output from an application/module to ensure that the processing of stored information is correct and appropriate to the circumstances.
5.	SI shall obtain information about technical vulnerabilities of information systems being used, evaluate the organization's exposure to such vulnerabilities, and take appropriate measures to address the associated risk.
6.	All systems / sub systems / applications that are acquired post go-live - whether COTS or developed by SI or procured by IAAD or developed by third party from SI or IAAD - shall also be assessed for security compliance prior to going into production.
7.	All changes that go into systems / sub systems / applications for bug – fixes / improvement / feature enhancement / performance related / etc. shall also be assessed for security compliance prior to placing in production environment or go - live.
8.	Segregation of Duties should be documented and monitored for access control and security requirements.
F	**Information security incident management**
1.	SI shall prepare the information security incident management process and the same will be approved by IAAD.
2.	SI will report and handle all the security incidents as per the timelines and action defined in the process document.
3.	All the critical security incidents need to be reported and responded within 60 mins of identification.
4.	SI will deploy appropriate technologies to detect and proactively response to security incident. These technology solutions will include the following:

A.	Information Security Management System (ISMS) – ISO 27001 Certification
	a) Antivirus solution: SI will deploy antivirus solution for DC/DR infrastructure, wherever required. b) Anti-Spam and Email security: - SI will deploy antispam and gateway antivirus and email security solution – if and where needed. The mail services are only for the purpose of sending system generated mails/notifications etc. to users. The system is not envisaged to host any mailboxes or any Incoming mails in to the system. All necessary security features with respect to these messaging requirements need to be assessed & provisioned by the SI as per his solution. c) IDS/IPS: - SI will deploy IDS and IPS solutions for security incident identification and prevention. d) Firewall: - SI will deploy firewall to create various zones within the data center. These will include at the minimum a DMZ, Production zone, Test and Development Zone, and security zone (MZ) with in the data center and at DR site.
G	**Security Compliance**
1.	SI will ensure that all infrastructure, systems, sub systems, middleware, firmware and applications comply with the applicable IAAD policies, IT Act and CERT-In guidelines during the contract period.
2.	No unlicensed software, shareware, public domain software or pirated software will be used.
3.	It is the responsibility of SI to ensure that any commercial software acquired, is used only in accordance with licensing agreements. Likewise, it is also their responsibility to ensure that any proprietary software is properly licensed before being installed in the OIOS environment. IAAD does not permit the usage of: a) Unlicensed commercial software b) Any Reversed Engineered -Cracked Software

A.	Information Security Management System (ISMS) – ISO 27001 Certification
4.	SI should provide and reconcile all licenses with software installed/utilize. SI should maintain this inventory or audit of licenses in electronic and paper repository which shall be in the custody of IAAD.
5.	SI should also ensure that all updates, upgrades of all prescribed licenses software are obtained and installed on a regular basis. Updates, upgrades to be mandatorily taken for all security and network components.
6.	SI shall execute all IT operations through detailed documented ITIL processes, procedures, SOPs, and work instructions including but not limited to Capacity Management, Availability Management, Problem Management, Identity and Access Management etc.
7.	Compliance to Processes shall be measured as an SLA. Violations to processes discovered during internal / third party / security / independent audits would invite penalties as applicable
8.	SI shall also ensure the vulnerability assessments of all systems / sub systems / network devices and appliances. Frequency of assessment shall be half yearly.
9.	SI should perform the Penetration Testing for all internet facing systems / sub systems. Frequency of assessment shall be yearly.
10.	SI also need to ensure the Patch management of all systems/ subsystems / network/ appliances/software as part of the security processes with OEM defined timelines for high, medium, low categories.
H	**Security Personnel**
1.	SI will ensure that qualified and competent Security resources with relevant experience are deployed as part of the team during the complete contract period i.e. implementation and operation stage.

A.	Information Security Management System (ISMS) – ISO 27001 Certification
2.	The Personnel should have adequate experience, education and experience in the field of Information security. Information security experience (as per RFP vol-I) resource should be deployed as part of the team.
I	**Asset Management**
1.	SI will prepare the information asset register (IAR) for all the assets deployed. The IAR will capture criticality, rating, classification, owner, custodian of the IAR.
2.	SI shall develop and implement an appropriate set of procedures for information labeling and handling in accordance with the classification scheme adopted by IAAD.
3.	SI will also prepare asset register which will capture the physical assets along with serial number, model, make, location and other details to track the asset. SI should have a CMDB (Configuration Management Database) to manage and track and audit the configurations of all assets deployed for OIOS.
4.	All the assets will be marked as per the asset identification guideline by the SI. The asset identification code will follow a defined naming convention that would uniquely and appropriately identify the asset. The asset inventory database should have a unique id. Each asset should be trackable through this unique id through its entire life cycle and deployment in the OIOS project.
J	**Physical and Environmental Security**
1.	SI will ensure that all items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
2.	SI will ensure that all the equipment, information or software shall not be taken off-site without prior authorization of IAAD.

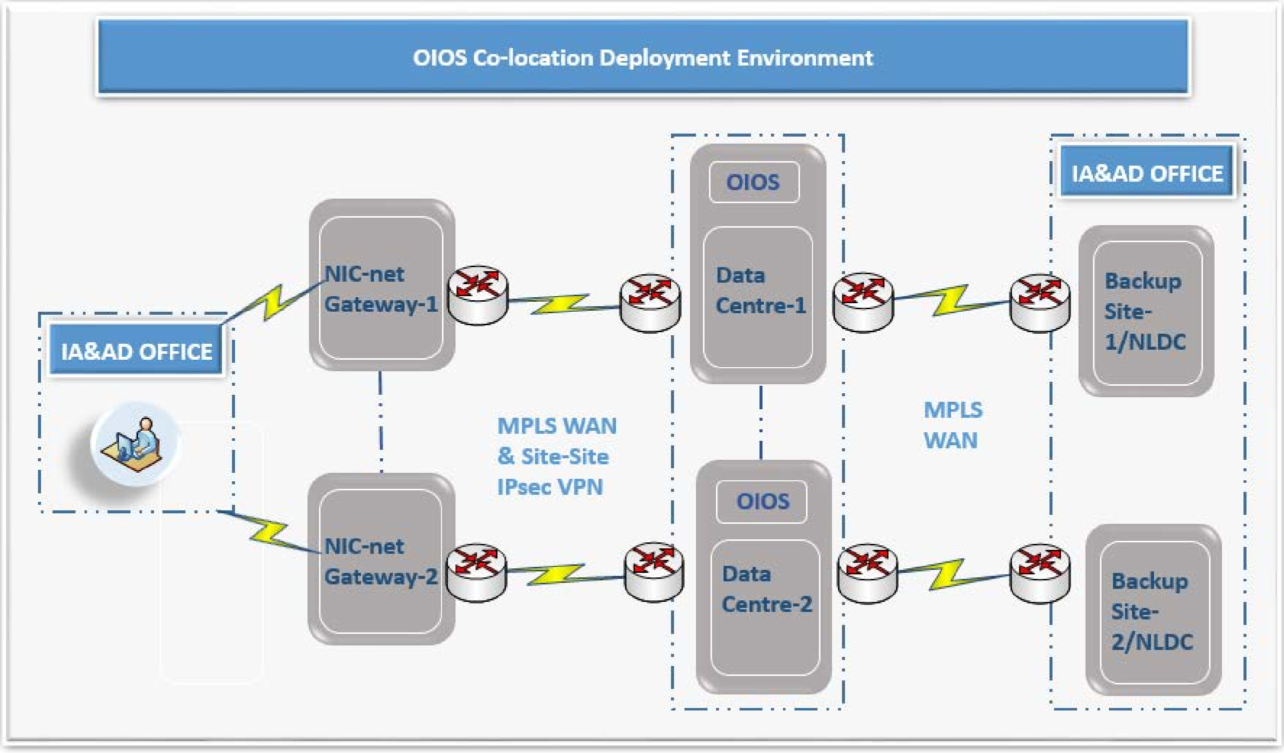
A.	Information Security Management System (ISMS) – ISO 27001 Certification
3.	All risks associated with physical and environment security will be owned by SI.

5. Business Continuity Planning and Disaster Recovery

1. SI would prepare the Business Continuity Plan for the OIOS Application in compliance with ISO 22301:2012 - Business Continuity Management System and submit the necessary documentation to IAAD.
2. The purpose of business continuity/disaster recovery is to enable OIOS to continue offering critical services in the event of a disruption and to survive a disastrous interruption to activities.
3. As stated in the SLA (Annexure to Volume- III) of this RFP, the SI shall design the OIOS solution architecture for OIOS Application and associated Services so as to ensure the following parameters:

Objective	Duration
RTO	4 hours
RPO	15 minutes

4. In order to achieve above SLA parameters for OIOS Application and to ensure business continuity, SI would set-up a Secondary Data Centre. Both the Data Centres (Primary and secondary) would be hosted in co-location option. IAAD reserves the right to migrate the OIOS data/application hosted at (either or both) data centres to Cloud Data Centres at a later date.
5. An indicative network Architecture is as follows:



6. The components of above are as follows: -

    a) Primary Data Center

    b) Secondary (Disaster Recovery) Data Center

    c) Near line Data Center (NLDC-1)/ equivalent backup site in same city as of PDC

    d) Near line Data Center (NLDC-2)/ equivalent backup site in same city as of DR DC

7. Primary Data Center: PDC shall host all OIOS components. SI shall deploy OIOS Application and its system software components as per Project Phases defined in RFP Vol-I.

8. Secondary (Disaster Recovery) Data Center: Disaster Recovery services will be provisioned in order to ensure continuity of OIOS services for longer duration disruption in PDC services. Resuming of services from DR site within specified time i.e. RTO will ensure availability of OIOS application services.

9. The Disaster Recovery Data Center shall have the following minimum specifications:

    a. **Compute Size:** 50% of Primary DC

    b. **Storage:** Same as Primary DC

10. Near line Data Center: NLDC shall have minimum of SAN, UPS to support SAN and backup software. SI needs to propose NLDC/ equivalent backup site components. NLDCs need to be located in the same city as of DC-1, DC-2. SI should propose BoM so as to meet specified RTO, RPO and other KPIs from SLA. IA&AD shall provide space and other arrangements for hosting necessary equipment.
11. SI shall adhere to the BCP/ DR requirements as specified in this Document.
12. The Primary Data Center (DC-1) and Disaster Recovery Site (DC-2) are to be set up in different locations so as to mitigate the risk of both sites being affected by location-specific threats.
13. Disaster Recovery Site should not require configuration changes for switchover from the Primary Data Center to Disaster Recovery Site.
14. Further, DR drill to test such switchover functionality shall be done. This would help to gauge the state of readiness of various other processes and procedure relating to business continuity and disaster recovery that may not get tested in a planned exercise.
15. **DR Drills/Testing:**
    a. Business continuity plans must be tested. DR drills should be conducted on a six-monthly basis.
    b. A test schedule should be drawn up for the business continuity plan. The schedule should indicate how and when each element of the plan would be tested.
    c. The drill should include running all operations from Disaster Recovery Site for at least 01 full working Day.
    d. Before DR drills, the timing diagrams clearly identifying resources at both ends (Disaster Recovery Site as well as Data Center) should be in place.
    e. The results and observations of these drills should be documented and placed before IA&AD.
    f. Feedback from the tests should be used to update the plans.
    g. The SI would communicate the results of the DR drills and any changes in the BCP to IAAD after each test.

SN	Features	Availability (Y/N)	Remarks
1.	OIOS solution should be architected to run on one data center facility to provide business continuity as per defined RPO and RTO and SLA.		
2.	In case of disaster at Primary DC site (within the defined RTOs and RPOs), the DR should be available (with its data) on-demand basis, wherein 100% of the services of Primary DC would run from DR site (after the RTO time and with the RPO level). Once the DC is restored, failback to DC is to happen.		
3.	SI should size solution as per defined RPO and RTO and SLA. DR should be available at time of disaster at Primary DC.		
4.	**SI shall define and submit (as part of the solution), a detailed approach for “Business Continuity Planning**”; this should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster; further, it should define the parameters at which “disaster” would be declared.		
5.	BCP should have minimum four main components: Emergency procedures – describing the immediate action to be taken following a major incident that jeopardizes business operations. Fallback procedures – describing the action to be taken to move essential business activities or support services to temporary locations. Resumption procedures – describing the action to be taken to return the business to the normal full operation, usually at the original site. Test schedule – which states how the plan should be tested.		

SN	Features	Availability (Y/N)	Remarks
	Each level of plan, and each individual plan, should have a specific custodian. Copies of each of the above business continuity plans should be held off site.		
6.	The SI should have a practicing framework for business continuity planning and the plan development which has been established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.		
7.	The SI should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes.		
8.	Incident response plans should be developed by the SI which should include impacted users and other business relationships that represent critical business process dependencies.		
9.	In case of failure, automated/ manual processes should resume services from DR site. The SI would ensure that adequate bandwidth between the Data Centre Facilities to provide business continuity.		
10.	SI should offer switchover and switchback of individual applications (from services standpoint) apart from the entire system.		
11.	In case of failover to DR site (once disaster is declared), the SLA performance parameters would not be applicable for RTO period only. The DR Site should take over the operations within the RTO period. Post RTO period, all SLA parameters (with exception to parameters for CPU and RAM utilization) would be applicable.		

SN	Features	Availability (Y/N)	Remarks
12.	The SI would be responsible for identifying and applying changes to the BCP. Individual changes should be applied periodically. The complete plan should be reviewed at least annually.		
13.	Awareness & Training – SI would conduct training(s) to make aware the personnel involved in Disaster Recovery Process about the contents of BCP, together with the duties and responsibilities of each party.		

6. Data Center Management

This section of the document describes various Service requirements of the IAAD and specifies a list of features for the Data Center which have to be part of the OIOS solution. The additional security requirements for the SI have been stated further in this Document.

6.1. Assumptions: Data Center Indicative Sizing

This section provides indicative sizing requirement for the OIOS Application. This assessment has been done by IAAD based on the number of expected users and volume of audit products (reports). The SI is required to carry out independent assessment of sizing requirement and propose solution accordingly.

The performance of the OIOS Application would be driven by the performance parameters stated in the SLA. Any variation between actual and indicative sizing would not confer SI any right to seek deviation(s) from the performance parameters stated in the SLA.

6.1.1. Server Sizing

Server sizing: OIOS at DC-1 (Primary DC)

Sl.	Services	User	Accessible on	No of estimated users	Concurrency	User Load	Cores required	RAM (In Gb)	Phase	Deployment Zone	Remarks
1	**Services**										
1.1	**OIOS - HQs, Field offices**										
1.1.1	Portal	CAG Offices	Internet	8700	10%	870	8	32	I	DMZ	
1.1.2	Application with workflow	CAG Offices	Intranet	8700	10%	870	16	64	I	MZ	
1.1.3	Database	Application	N.A.				16	64	I	MZ	
1.1.4	Document server	Application	N.A.				8	32	I	MZ	
1.2	**OIOS - Auditors at Field**										Sizing covered at 1.1
1.2.1	Portal	CAG Offices	Internet	20300	2%	406				DMZ	
1.2.2	Application with workflow	CAG Offices	N.A.	20300	2%	406				MZ	
1.2.3	Database	Application	N.A.							MZ	
1.2.4	Document server	Application	N.A.							MZ	
1.3	**GIS**										
1.3.1	Map engine	Application	N.A.				8	64	II	MZ	
1.3.2	Database	Application	N.A.				4	64	II	MZ	
1.4	**Media news**										
1.4.1	Application	CAG Offices				-	4	32	II	MZ	
1.4.2	Search engine	Application	N.A.				16	128	II	DMZ	
1.4.3	Database	Application	N.A.				2	32	II	MZ	
1.5	**System component**										
1.5.1	Document Mgmt. System	CAG offices	Intranet, Internet								Covered in 1.1.4
1.5.2	Knowledge Mgmt. System	CAG offices	Intranet, Internet				8	32	II	MZ	
1.5.3	Discussion forum	CAG offices	Intranet, Internet				8	32	II	DMZ	
1.5.4	BPM	Application	N.A.				8	32	I	MZ	
1.5.5	Identity management - internal users	Application	N.A.				4	16	I	MZ	
1.5.6	Messaging server forwarder	Application	N.A.				4	16	I	MZ	
1.5.7	Privilege access management	Application	N.A.				4	16	I	MZ	
1.5.8	Helpdesk	IA&AD offices	Intranet, Internet							MZ	Handled at Application level

Sl.	Services	User	Accessible on	No of estimated users	Concurrency	User Load	Cores required	RAM (In Gb)	Phase	Deployment Zone	Remarks
1.6	**System Monitoring**										
1.6.1	APM	OIOS Monitoring Cell	Intranet				8	32	I	DMZ	
1.6.2	EMS	IT Monitoring Cell	Intranet				16	64	I	MZ	
1.6.3	SIEM	IT Monitoring Cell	Intranet				32	128	I	MZ	
1.6.4	SLA monitoring	IT Monitoring Cell	Intranet				2	4	I	MZ	
1.6.5	DNS	IT Monitoring Cell	Internet				4	8	I	MZ	
1.7	**Reporting**										
1.7.1	Reporting	Auditors	N.A.	1,400	1.00%	14	8	32	II	MZ	
1.7.2	IA&AD's analytics tool						32	128	II	MZ	MZ/DMZ
1.8	**Auditee Data repository**										
1.8.1	Portal, Database instance	IT Cell	N.A.	140		-	4	16	II	DMZ	
1.8.2	Auditee data dump conversion	CAG Offices	N.A.			-	20	80	II	MZ	
1.9	**Non production servers**										
1.9.1	Development environment						64	256	I	DMZ	MZ/DMZ
1.9.2	Testing						64	256	I	DMZ	MZ/DMZ
1.9.3	Training						16	64	I	DMZ	MZ/DMZ
1.9.4	Pre Production						64	256	I	DMZ	MZ/DMZ

Summary: DC-1	
Zones	Cores
MZ	200
DMZ	252

Server sizing: DC-1 (Primary DC)

The sizing for DC-1 is as follows:

Total Cores: 452 (MZ: 200 cores, DMZ: 252 cores). Out of which:

a. Development, Training, Testing environment: 208 Cores

b. Production environment: 244 Cores

Server sizing: DC-2 (DR)

DC-2 must have at least 50% compute of DC-1 (production environment) ~ 128 Cores (i.e. 4 Blades of 2X16 Cores) [rounded-up from 122 cores].

However, SI need to propose size DC-2 as per requirement specified in BCP & DR section.

Note:

1. Cores specified here are x86 Core.
2. Server Sizing would change based on the key data indicators (Annexure -D RFP Vol-1)

6.1.2. Storage sizing

Estimated Key Document sizing (per year)

Nature of assignment	Number of assignments	Sizing per assignment[1]	Total sizing (Approximate)
Units covered under compliance audit assignments	56,692	50 MB	3.0 TB
Performance audit assignments	116	10 GB	1.0 TB
Financial audit assignments	8,260	50 MB	0.5 TB
		Total	**4.5 TB**

Estimated Audit products sizing (per year)

Nature of assignment	Number of assignments	Sizing per assignment[2]	Total sizing (Approximate)
Inspection reports	48,106	10 MB	0.5 TB
Audit reports	98	50 MB	0.05 TB
Audit certificates	8,260	10 MB	0.1 TB
		Total	**~1 TB**

Estimated Data sizing:

Description	Sizing per year	Sizing for hardware estimated life (07 years)
Key document sizing	4.5 TB	31.5 TB
Audit product	1.0 TB	7.0 TB
Total	**5.5 TB**	**38.5 TB**

Storage sizing: DC-1:

- DC-1 Storage sizing ~ 40 TB usable (rounded up) upgradable to 60TB.

Storage sizing: DC-2 (Secondary or Disaster Recovery DC)

- SI need to size DC-2 as 100% (Same size) as Primary DC.

6.2. Features for Data Centers (DC/DR)

6.2.1. DC/DR Services - General Features

SN	Features	Availability Y/N	Remarks
1.	SI shall assess the infrastructure requirements including Number of VMs, OS Instances, Storage, DC Networking, Security etc.) for hosting and maintaining all required applications/services. The SI shall provide the services in conformance with the SLAs as described in the RFP.		
2.	The SI should ensure that all peripherals, accessories, sub-components required for the functionality and completeness of the OIOS solution, including but not limited to devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution. IA&AD will not be responsible if the SI has not provisioned some components, sub components, assemblies, and sub-assemblies as part of bill of material in the bid. The SI will have to provision the same to meet the solution requirements at no additional cost and time implications to IA&AD.		
3.	The SI should use Open Source Solution (Enterprise Edition) for any system software that SI would be using. In case there is a need to purchase/ provision COTS (Commercial-off-the-Shelf) license, the same should be flagged and justified.		

SN	Features	Availability Y/N	Remarks
	Additionally, any purchase of any license or support should be in the name of IA&AD. The support for system software shall be provided for full Project duration: a) Open source software: Enterprise OEM support COTS: ATS-Enterprise OEM support/ ATS		
4.	The bidder should specify DC and DR locations.		
5.	SI should provide (direct leased-line connections between DC/DR) and IAAD’s NICNET gateway since the connectivity for IA&AD is provided by NICNET across all offices. Further, SI is to size the bandwidth requirements for the same. SI is required to discuss the connectivity with NIC and choose the network accordingly.		
6.	OIOS Solution and its services should be accessible via internet and IA&AD NICNET.		
7.	It is expected that the SI will provide an integrated solution, after due consideration to the compatibility issues between various components. If there is a problem with compatibility between components, the SI should replace the components with an equivalent or better component (that is acceptable to IA&AD) at no additional cost to IA&AD and without any project delays.		
8.	SI should use REST based Open API for each of the services for automation along with SDKs for platforms like Microsoft .net, Java/JavaScript, Python, PHP or Ruby. The SI should be able to utilize these API's to set up routine jobs such as backup on an automated schedule wherever necessary.		

6.2.2. OIOS Services - Policy Features

SN	Features	Availability (Y/N)	Remarks
1.	The DC DR Infrastructure must be maintained ONLY at the declared hosting site which should be communicated as part of the solution document.		

6.2.3. Logical Partitions features

SN	Features	Availability (Y/N)	Remarks
1.	All the applications would follow a three-tier architecture with clear separation of database tier/layer from application and web layers. For micro services-based architecture, SI should deploy Presentation, Logic and Database category of micro services on different VM's/Containers.		
2.	The Web layer for applications accessed via Internet/MPLS WAN shall be hosted in the DMZ zone; the application layer should be hosted in the Militarized Zone.		
3.	The Database nodes (RDBMS) should be in a MZ.		

SN	Features	Availability (Y/N)	Remarks
4.	All management servers which are not directly accessible through the internet will be kept in MZ. Directory server, EMS, APM, SIEM, Different modules of Enterprise Management Servers (including network, server, database, helpdesk etc.), Single-Sign-On, access and identity management server, etc., will be a part of this MZ.		
5.	There will be separate VLANs/Subnets created for Training, UAT and Production environment to segregate traffics from the production. Appropriate firewall policies can be implemented to have further security between different zones.		
6.	For the purpose of sizing, the SI would size the solution on User Acceptance Testing (UAT), Training, and Production Environment. High availability, if necessary, to be provided as specified in respective component for Production environment only.		

6.2.4. Configuration features

SN	Features	Availability (Y/N)	Remarks
1	The SI shall ensure that identity solution is utilized and use best practices like least privilege, secure delete, enable Multi Factor Authentication for users.		

6.2.5. Service features

SN	Features	Availability (Y/N)	Remarks
1.	All services of OIOS should be managed from a single console.		
2.	Able to define guidelines for provisioning and configuring compute/ services resources and then continuously monitor compliance with those guidelines.		
3.	Provide Audit logs of the account activity to enable security analysis, resource change tracking, and compliance auditing.		

6.2.6. Incident Response features

SN	Features	Availability (Y/N)	Remarks
1.	The SI should have policies and procedures in place for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. The SI must also have policies and procedures in place to ensure timely and thorough incident management, as per established IT service management policies and procedures.		
2.	The SI must bring in an ITSM tool through which the tickets (for incidents or other issues) can be logged in.		
3.	The SI should have proper forensic procedures defined and implemented, including chain of custody, required for the presentation		

SN	Features	Availability (Y/N)	Remarks
	of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.		
4.	A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.		

6.2.7. Governance & Risk Assessment features

SN	Features	Availability (Y/N)	Remarks
1.	The SI should have organizational practices in place for policies, procedures and standards for application development and service provisioning as well as design, implementation, testing, use, and monitoring of deployed or engaged services.		
2.	SI would develop audit plans for security policies, procedures, standards, and controls taking the business process disruptions into consideration. Audit plans shall focus on reviewing the effectiveness of		

SN	Features	Availability (Y/N)	Remarks
	the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.		
3.	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.		
4.	Solution shall have an audit and compliance features which enables the Client agency to monitor the provisioned resources, performance, resource utilization, and security compliance.		
5.	The solution should have security assessment that should provide the following: a. vulnerabilities assessment b. Penetration Testing c. deviations from best practices such as password policy, unnecessary opened firewall ports, storage access policy, suggestion of data to archive		
6.	The system should have ability to set up alarms for high resource usage and the ability to define actions on triggering of those alarms (For example, ability to send an email when storage utilization has crossed x% or archive a storage section depending upon data type when it has crossed x% utilization)		
7.	Visibility into the performance and availability of the services being used, as well as alerts that are automatically triggered by changes in the health of those services.		

SN	Features	Availability (Y/N)	Remarks
8.	The solution should provide a dashboard that would list the details of any planned maintenance scheduled as well as any unplanned downtime faced in the recent past (past 3 months at least).		
9.	SI should provide dashboard for monitoring RPO and RTO. The Dashboard should clearly show data replication process and any lag/ failure in data replication that should be notified through alerts to respective authorities.		
10.	The solution should be able to log all account and resource access into the account and resources (which might be resources logging into the account using API call or root/admin users or other users logging into the account).		
11.	The solution should be able to discover all provisioned resources and provide details such as configuration items inventory, history of changes to such configuration items, snapshot of resource inventory at a single point in past, set-up of policies to track provision of resources within a client defined rulesets and auto-notifications each time a configuration change.		
12.	The solution should be able to suggest best practices to optimize overall cost of resources.		

6.2.8. Compute features

SN	Features	Availability (Y/N)	Remarks
1.	The system must be Scalable, Reliable, Highly Available & should provision to upgrade/downgrade virtual machine configuration (vCPU, vRAM, storage) parameters seamlessly.		
2.	In order to meet SLAs, SI may implement high availability options for OIOS Application (production environment): a) RDBMS b) Web and Application server		
3.	The SI shall ensure that the services that are deployed on partitions/virtual images and are required in cluster and/or load balancing mode, shall be deployed in such a manner that the load sharing/failover is across the OS instances and NOT amongst partitions of the same OS instance. In case of a hardware or software component failure in one partition, other partitions must not be shut down or rebooted.		

6.2.9. DC Networking features

SN	Features	Availability (Y/N)	Remarks
1.	Service should ensure logical isolation of the infrastructure.		
2.	SI should support the ao create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.		

SN	Features	Availability (Y/N)	Remarks
3.	The SI should provide mechanisms to establish client VPN between the DC DR environment and a stakeholder office(s).		
4.	OIOS service should support Load balancing (local) of instances across multiple host servers.		
5.	OIOS service should support multiple routing mechanism including round-robin, failover, sticky session etc.		

6.2.10. Storage features

SN	Features	Availability (Y/N)	Remarks
1.	Should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies. There should be an option to choose the media type with respect to the type of environment. The indicative disk type is as follows: a) OIOS Production RDBMs instances: SSD b) Data repository RDBMs instances: SSD c) Analytics RDBMs instances (Active): SSD d) Data repository RDBMs archival: SAS/ NLSAS		
2.	The Storage should support a low-cost storage disks that provides durable storage with security features for data archiving and backup.		

6.2.11. Backup features

SN	Features	Availability (Y/N)	Remarks
1.	The SI should offer a service with ability to take regular and scheduled backup.		
2.	The SI should propose Software deployed on VM based backup software.		
3.	Low cost Object Storage should be utilized as the backup target. If there is need to use the block-based storage for backup target for staging or as a whole, the same should be flagged and explained.		
4.	The SI shall prepare and submit a back-up plan to IAAD detailing how the SI would configure, schedule and manage backups. The backups would consist of all the data including but not limited to files, folders, images, system state, databases and enterprise applications a) An Initial Full Backup b) Daily Incremental with 15-day retention c) Weekly full with 30 days retention d) Monthly Full with 30 days retention on Object Storage and 12 months retention on Long Term storage e) Yearly Full with 30 days retention on Object storage and 5 Years retention on Long term storage f) For the databases, perform a twice weekly full database backup with a three times daily backup of database log files g) Encryption of all backup files and data and management		

SN	Features	Availability (Y/N)	Remarks
	h) Different Tiers of Backup storage should be chosen depending upon the reads/restore that would be required i) Restoration Policies: • Backups taken in last 2 months: Once in a month • Backups taken in last 6 months: Once in a Quarter • Backups taken in last 1 Year: Once in Half Year The restoration would be performed on a random basis and would be done against a ticket logged in the ITSM tool.		

6.3. Data Center Connectivity to NIC gateways and mobile users

6.3.1. Existing IT Networking Infrastructure of Field Offices

IA&AD field offices across India have engaged MPLS WAN from various service providers to provide network connectivity (intranet/ internet) to its employees. IA&AD Offices are inter-connected using NIC network through MPLS WAN (Leased Line). The bandwidth availability of NICNet at IAAD field offices varies between 10 Mbps to 1 Gbps.

6.3.2. Network Connectivity: DC to IA&AD NICNET & NLDC/ Backup Sites

To ensure accessibility of the OIOS application by users and to meet the application data replication requirements between all DCs i.e. both data centres and both Backup sites, SI shall provide the MPLS Connectivity to meet the required RPO and RTO. This shall include:

a) Connectivity between Data Centre-1 to:

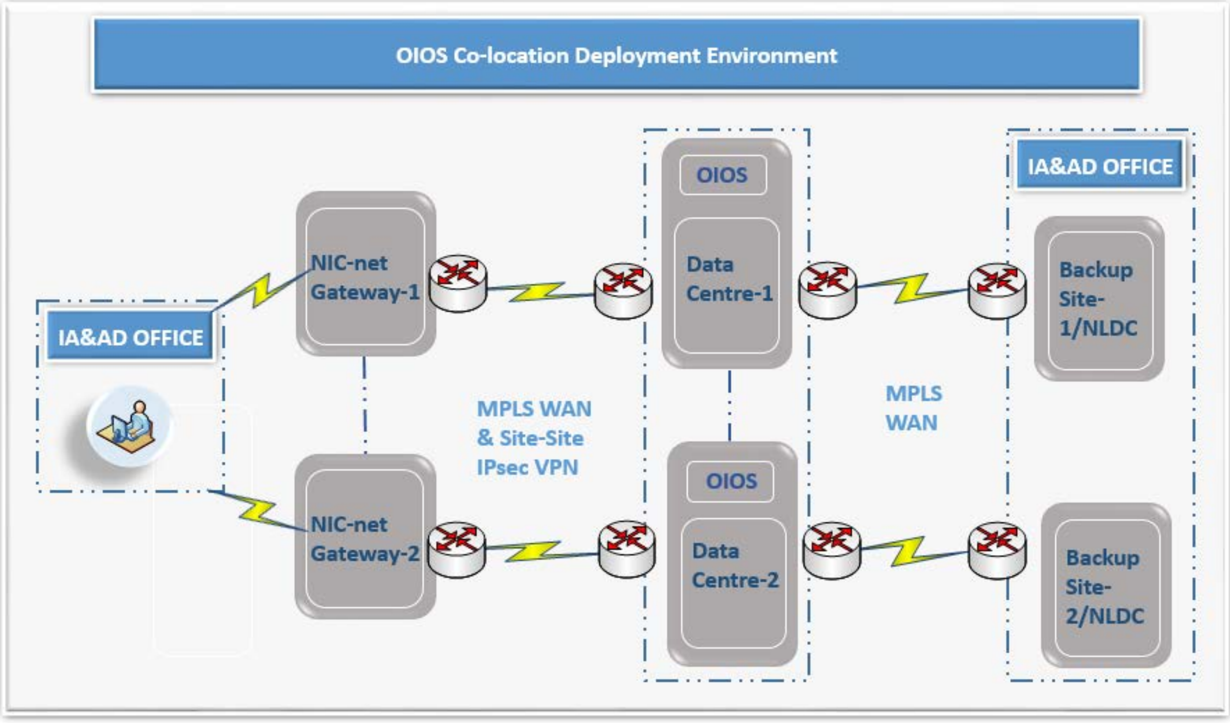
- IA&AD NIC-net Gateway 1.

- Backup Site-1/NLDC to hold only data backup for achieving desired RPO. No other compute infrastructure except storage, SAN is envisaged to be hosted at Backup sites.

b) Connectivity between Data Centre-2 to:

- NIC-net Gateway 2.
- Backup Site-2/NLDC.

c) SI shall ensure dedicated high speed connectivity between DC-1 and DC-2.



Bandwidth requirement of OIOS:

Users shall access OIOS Application as following:

Case 1: IA&AD staff at field offices (HQ, AG office, Branch Office, DG/ PD office) would connect to Data Center through NIC gateway (NICNet).

The connection between the field offices to NIC gateway is via dedicated lease lines and is outside the scope of SI. The SI has to ensure that appropriate bandwidth is made available tot OIOS Application at NIC Gateways so that the users can access OIOS Application seamlessly.

Assumption: IAAD has esimated that a total of 8700 users at IAAD field offices (HQ, AG office, Branch Office, DG/ PD office) would be accessing OIOS application from Offices at a concurrency of 10%.

Indicative bandwidth requirement as per IAAD estimation is shown in following table:

From	To	Bandwidth requirement in Mbps	Number of links
DC-1	NIC-Net Gateway- 1	100	1
DC-2	NIC-Net Gateway- 2	100	1

Note: SI should provide direct leased-line connections between DC/DR and NICNET keeping in view that the connectivity for IA&AD is provided by NICNET across all offices. The SI is required to carry out independent assessment of bandwidth requirement and discuss the same with IA&AD's NIC representative. The performance of the OIOS Application would be driven by the performance parameters stated in the SLA. Any variation between actual and indicative bandwidth reuirement would not confer SI any right to seek deviation(s) from the performance parameters stated in the SLA.

Case 2: Audit party (users) in field would connect to Data Center using Mobile data internet or NIC gateway (in certain cases).

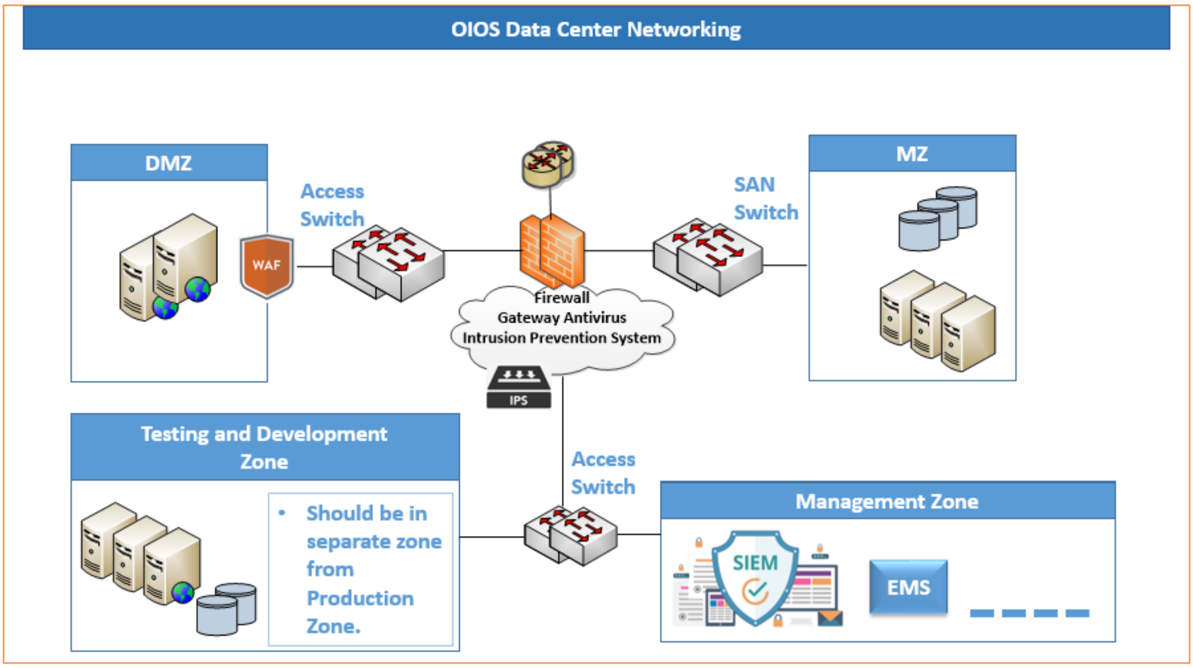
Assumption: IAAD has esimated that a total of 20300 field party users would be accessing OIOS application through mobile internet connection at a concurrency of 2%.

Note: SI should design OIOS solution keeping in view that the application is available to mobile users through mobile internet connection with/without VPN. The SI is required to carry out assessment of bandwidth requirement and discuss the same with IA&AD's NIC representative.

Connectivity between Data Centers and NLDCs:

From	To	Bandwidth requirement in Mbps	Number of links
DC-1	Backup Site - 1/NLDC	SI need to size based on the data replication requirement	01 (Redundant link via NICNET to DC)
DC-2	Backup Site - 2/NLDC	SI need to size based on the data replication requirement	01 (Redundant link via NICNET to DC)

1. Proposed Data Center Architecture for OIOS is as below:


OIOS Data Center Networking
DMZ
WAF
Access Switch
Firewall
Gateway Antivirus
Intrusion Prevention System
IPS
SAN Switch
MZ
Testing and Development Zone
Should be in separate zone from Production Zone.
Access Switch
Management Zone
SIEM
EMS

The SI would ensure the following:

a. Provision of requisite bandwidth - This includes provisioning of internet at DC (DC-1), DR (DC-2); and Replication bandwidth. SI also needs to provide MPLS (leased line) connectivity to NICNet Gateways for Field Audit Offices.

b. To ensure the easy accessibility of the application by users, SI needs to provide the network connectivity as per the connectivity requirement mentioned below:

i. SI should provide the connectivity to meet the application data replication requirement between both Data Centers and both Nearline Data sites to meet the required RPO and RTO. This should include:

1. Connectivity between primary and secondary Data Centers.
2. Connectivity between Primary Data Centre and Nearline DC (NLDC-1).
3. Connectivity between Secondary Data Centre and Nearline DR (NLDC-2).
4. Connectivity solution to connect NLDC-1 and Secondary DC to recover the data in case of disaster/failure at Primary DC.
5. Connectivity solution to connect NLDC-2 and Primary DC to recover the data in case of disaster/failure at secondary DC.

ii. SI will also provide internet connectivity at primary and secondary data centers to allow access to OIOS Application from internet. Internet connectivity needs to be provided from two ISPs (from two different PoPs) at each Data center. The internet bandwidth should be provisioned to meet the user requirements.

c. Bandwidth estimation is to be done by SI based on the data replication requirement, user projections for entire contract duration and to comply with the service levels. Bidder needs to provide details of bandwidth sizing for each link in its technical proposal. Bidder may propose bandwidth in scalable model also. But at all times the SI need to meet the service levels as mentioned in this RFP.

d. SI shall provide the detailed Bandwidth calculation and should ensure that bandwidth utilization should not cross 70% at any point of time. During the operations if bandwidth utilization reaches 70%, SI will be required to increase the Bandwidth.

e. In its technical proposal the bidder needs to provide the details of bandwidth service provider (bandwidth service provider name) from whom it is going to provide bandwidth services.

f. The SI through EMS should also provide network related reports including the below:

i. Link up/down (real-time as well as periodic)

ii. Link utilization in % (real-time as well as periodic) (Link utilization should not be more than 70% in each case, barring acceptable occasional surges)

iii. Top and Bottom N graphs showing the best and worst links in terms of availability (periodic)

iv. Reports on threshold violations. Provisions for setting thresholds and getting alerts on threshold violations should be there in the system. (real-time as well as periodic)

v. Bandwidth utilization report for each link and utilization trends. The report should have provisions for displaying the minimum, maximum and average for each link. (real-time as well as periodic)

   a. The monitoring solution provides for application/port level traffic analysis with source and destination identifications

   b. Report on jitters, latency' due to network parameters, closely linked to reachability shall be available. (real-time as well as periodic)

   c. Router Statistics: CPU utilization and free memory reports of all the routers in the network should be available. Memory and CPU utilization reports will show maximum and minimum against a predefined threshold.

vi. The monitoring solution provides for application/port level traffic analysis with source and destination identifications.

vii. Report on jitters, latency due to network parameters, closely linked to reachability shall be available. (real-time as well as periodic)

Note:

1. Bandwidth estimation is to be done by SI based on the data replication requirement, for entire contract duration and to comply with the service levels. SI shall provide details of bandwidth sizing for each link in its technical proposal. SI may propose bandwidth in scalable model also. But at all times the SI needs to meet the service levels as mentioned in this RFP.

2. All the MPLS WAN links should have back up link to be provided from different service providers at each site i.e. from DC(s) to NIC-net Gateways and DC(s) to Backup sites etc. This is to

ensure two landings of network connectivity at each site. While links at each site are supposed to work in load sharing mode, the individual link for each location should be able to cater to the bandwidth requirement even if the secondary link is down. The redundant links at any location must not be overlapped on the same media by two service providers.

3. **NICNET is the primary WAN link and Internet provider used by IA&AD presently. However in case of change of WAN link provider/ addition of secondary WAN link by IA&AD, the provisioning of lease line from DC-1 & DC-2 to new gatway shall be changed.**

6.3.3. Network Connectivity features

SN	Features	Availability (Y/N)	Remarks
1.	All the MPLS WAN links should have back up link to be provided at each site i.e. from DC(s) to NIC-net Gateways and DC(s) to Backup sites etc.		
2.	In its technical proposal the SI shall provide the details of bandwidth service provider (bandwidth service provider name) from whom it is going to provide bandwidth services.		
3.	The SI through EMS should provide network related reports amongst other the following: i. Link up/down (real-time as well as periodic) ii. Router up/down (real-time as well as periodic) iii. Top and Bottom N graphs showing the best and worst links in terms of availability (periodic) iv. Reports on threshold violations. Provisions for setting thresholds and getting alerts on threshold violations should be there in the system, (real-time as well as periodic) v. Bandwidth utilization report for each link and utilization trends. The report should have provisions for displaying the		

SN	Features	Availability (Y/N)	Remarks
	minimum, maximum and average for each link. (real-time as well as periodic) a. The monitoring solution provides for application/port level traffic analysis with source and destination identifications b. Report on jitters, latency' due to network parameters, closely linked to reachability shall be available. (real-time as well as periodic) c. Router Statistics: CPU utilization and free memory reports of all the routers in the network should be available. Memory and CPU utilization reports will show maximum and minimum against a predefined threshold.		

6.4. Performance Management and Monitoring:

Performance Management involves monitoring, collecting the required resource utilization metrics and tuning of virtual resources. In addition, in a High Available virtual environment, devices can be added, removed and load balanced for managing the required levels of performance. Also, configurations of the logical partitions and virtual environments may be tuned for performance optimization. Processes may also be moved seamlessly to maintain the levels of performance.

The EMS module of the OIOS Application should be able to monitor the set of performance objectives for the SI. Typically, this set of objectives includes system and security resources such as CPU, Memory, process, storage and High Available service, utilization, configuration changes or any other parameters. The SI has to do the following:

1. Perform the virtual environment/device availability monitoring
2. Perform the virtual device alert monitoring
3. Perform the configuration change and log monitoring
4. Monitor the virtual device access to ensure the continuous CIDR operation

5. Monitor the performance of the virtual server/ device and highly available systems
6. Monitor the utilization of resources (CPU, Memory, Storage) and network connectivity
7. Monitor the physical server capacity and distribution of virtual servers
8. Proactive identify security vulnerabilities and potential threats

7. Minimum Specification of IT infrastructure for OIOS Solution:

The specifications given below are only indicative in nature. The proposed systems and IT Infrastructure components like Servers, Storage, Network etc. should be of enterprise class and must be current as per OEMs latest offering, in line with advancements of technology in these domains. Bidder needs to provide the published benchmarks for the stated systems along with the sizing assessment sheet certified by the OEM for the stated systems. All the components should be able to handle expected loads and provision the desired transaction times and throughputs.

7.1. DevOps Environment

Deployment of applications or application changes/components etc. in OIOS with complex/layered architecture needs a seasoned deployment process and tools. It is recommended to use advanced capabilities such as DevOps which has capabilities of continuous integration and continuous deployment to reduce the time it takes a change in development and move the change to production.

SN	Features	Availability (Y/N)	Remarks
1.	SI should offer solution for DevOps consisting of: a. Coding – code development and review, source code management tool, code merging b. Building – continuous integration tools, build status c. Testing – continuous testing tools for quick and timely feedback (Automated testing shall be preferred)		

SN	Features	Availability (Y/N)	Remarks
	d. Packaging – artifact repository, application pre-deployment staging e. Releasing – change management, release approvals, release automation f. Configuring – infrastructure configuration and management, infrastructure as code tools g. Monitoring – applications performance monitoring, end-user experience		
2.	Solution should include Repository, Build & Deployment Tools, and Agile planning tools.		
3.	To create a reliable CI/CD pipeline, practice "infrastructure as code" and continuous monitoring.		
4.	DevOps solution shall provide security and monitoring.		
5.	Version Control of all Production Artifacts: Both Dev and Ops should use version control and share the same single source of truth.		
6.	Provision of dev-test environments directly from continuous integration (CI) tools.		

7.2. Document Management System

An essential function of the OIOS Application includes managing, editing and retaining various versions of the draft Audit products (Audit reports). OIOS Application includes a Document Management Systems (also known as Content Management System) as a component of Enterprise Content Management (ECM).

The essential components of the DMS include:

- Simultaneous but separate editing of documents to avoid the conflict of overwriting.
- To roll back to the last accurate version of the document in case of any error.
- Version control to differentiate between two different versions.
- Reconstruction of documents.

In addition to the above features, the DMS is expected to contain other components such as Security and Access Control, providing audit trail, Indexing, Classification, Search, Retrieval and Integration with other applications.

The SI has to submit that the proposed DMS complies with above components. An indicative list of DMS features is as follows:

SN	Features	Availability (Y/N)	Remarks
1.	The OEM should fall in the Gartner's magic quadrant for Content Service Platforms		
2.	The proposed DMS solution must have both the options of saving images in image/file server and store metadata information in database.		
3.	Support open, scalable, Multi-tier architecture with each tier fully independent with support for clustering.		
4.	Inter-operability - The systems must seamlessly integrate with any or all of the existing legacy and Core applications and shall support interface with other open-standard systems.		
5.	Supported databases: offered OIOS database and other database formats (four additional RDBMS provided in BoM) supported by OIOS Application		
6.	Should provide an integrated scanning engine with capability for centralized and decentralized Scanning & Document Capturing.		

SN	Features	Availability (Y/N)	Remarks
7.	Should have a well-defined capture module for support of document processing, validation, index building, and image enhancements.		
8.	Should be able to support the capture of digital records of the (at least) following formats: • Emails and attachments • Images - .tiff, jpeg, gif, PDF etc. • Videos • Other formats for documents – word, xls, PDF etc.		
9.	Support all the special image enhancement functionality offered by the scanning solution.		
10.	Should have capability of automatic segregation of documents/records based on Barcode/QR Code, Blank page, Fixed page and auto Form recognition		
11.	Provide Image processing libraries that support image enhancements such as changing contrast, zoom in/out, cleaning etc.		
12.	The System shall support categorization of documents in folders-subfolders just like windows interface. There should not be any limit on the number of folder and levels of sub folder.		
13.	The system shall provide search facility in the same interface, so that users are able to search the documents to be linked. Search facility should include “Advance Search” and cataloguing the search results as – Primary (metadata/ title/ subject) and secondary (content).		

SN	Features	Availability (Y/N)	Remarks
14.	The system shall support versioning of documents with facility to write version comments		
15.	The System should have an inbuilt Document Viewer for viewing Image documents. The rendering of images should be page by page for quick viewing in the viewer.		
16.	The inbuilt Document Viewer shall support comprehensive annotation features like highlighting, marking text, underlining putting sticky notes on documents, and support for text and image stamps etc. without tampering the original document.		
17.	Support archival & view of PDF/A format documents (open ISO standard for long term archival of documents)		
18.	The system should support viewing and rendering of PDF/A documents in inbuilt viewer.		
19.	The System shall provide facility to index folders, files and documents on user-defined indexes like Department, Ministry, file number, year etc.		
20.	The System shall support Automatic full text indexing for Text search.		
21.	The system shall provide extensive search facility to retrieve documents or Folders/Files		
22.	The system shall support saving of search queries and search results		
23.	The Document management system shall support definition of Users, Groups and Roles relation in the system		

SN	Features	Availability (Y/N)	Remarks
24.	The system shall support access permissions on Folders, documents and object level		
25.	The system shall support multiple levels of access rights (Delete/ Edit/ View/ Download).		
26.	The system shall provide LDAP support for integrating with directory services and shall support single sign on		
27.	The system shall support Extensive Audit-trails at document, Folder and for highest levels for each action done by particular user with user name, date and time		
28.	The proposed system should have "Out of the Box" integration capability with popular office software e.g. word, xls, ppt etc. No third-party add-ons should be used to meet such functionalities.		
29.	Must provide CMIS and REST API support		
	The proposed DMS solution should not impose any OEM specific proprietary encryption while saving the images and binary documents at storage level e.g. SAN/NAS etc.		
30.	The proposed DMs should have the option to download a file to local PC/laptop/mobile devices for offline editing and uploading the edited version to OIOS Application with version control.		
31.	The proposed DMS should have the option to download all/ multiple files as consolidated PDF file to local PC/laptop/mobile devices.		
32.	The zoom-in/out function for the documents should be advanced so as to allow fluidity in the line structure of the (word) document e.g. the		

SN	Features	Availability (Y/N)	Remarks
	zooming in a word file should restructure the line to accommodate with the new screen specification.		
33.	The DMS should allow highlighting any or all parts of a page in scanned pdf document and images. The solution should include linking the highlighted portions to one or multiple places in same or another document.		
34.	The proposed DMS should allow multiple linking of the documents e.g. one sentences/word may have multiple references.		

7.3. Business Process Management Software

The Audit process and documents flow differs significantly across streams of audit (Civil, Railways, Defence etc.), types of audit (compliance, financial, performance) and to some extent various offices (Civil Audit offices in Allahabad and Bengaluru etc.). The OIOS has to be designed to include configurability of business rules including policy decisions, business parameters etc. place within the system. The system shall provide facility to the decision makers to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace.

The proposed solution architecture would be flexible and would will make use of open standard workflow services (BPM) to allow authorized users to model and automate sophisticated business processes.

Few features (minimum requirements) that the proposed BPM solution should include:

a. Support easy workflow configuration, its maintenance, and need based modification, addition alteration of the steps.

b. Support process modelling based on BPMN2 notation standard.

c. Facility to simulate a process before launching it so that appropriate changes can be made based on findings.

d. Provide business rule engine and a management platform. Authorised users shall be able to modify the business rules online without any need of deployment. System shall also have business rule connector so that it can talk to any 3rd party business rule engine.

e. Allow saving custom BPM templates so that authorised user can tailor a business process based on any of the custom template.

f. Offer performance monitoring features for the business processes. The system shall be capable of identifying, reporting inefficient processes and operations and/or those with high level of error and omission.

g. Expose W3C standard web services and REST based web services so that it can communicate to any other technology layer seamlessly.

h. Have capabilities which will enable business activity monitoring and capture audit trail of all transactions as well. Web based dashboard shall be made available for accessing all reports.

i. Provide dashboard view for showing multiple reports. Dashboard view and content can be customized for individuals.

j. Visual workflow tool which allows the user to focus on the primary path of the business process and the software automatically handles the exception paths when operating. The user knows how the process should run every time and the system can offer the best way to structure the path.

Integration with External System: The BPM solution should allow API based integration with internal/external systems to OIOS.

The SI has to submit that the proposed BPM complies with above components. An indicative list of BPM features is as follows:

SN	Features	Availability (Y/N)	Remarks
1.	The OEM should fall in the Gartner’s magic quadrant for Intelligent Business Process Management Suites		
2.	Proposed BPM platform should support Database being offered for OIOS Application.		

SN	Features	Availability (Y/N)	Remarks
3.	Should support Windows, Linux, UNIX OS		
4.	BPM Solution must support the following kinds of processes: a) Human Workflows b) Integration Workflows (STP) c) Decision Centric Workflows d) Event Based Workflows e) Case Management based Workflows		
5.	The escalation and notification mechanism in the BPM solution should have support for: a) Email b) SMS		
6.	BPM Platform should have built in testing/simulation framework to test process end to end like Web forms, process flows, business rules while designing the processes		
Process Modeling			
7.	Web based modeling tool must be capable of handling Business Rules definition		
8.	Modeler be used for multiple levels of process model, starting from business process model for business users and analysts to executable process model for system architect.		

SN	Features	Availability (Y/N)	Remarks
9.	The solution should allow the running process instance to be stepped back, when needed, without having to redeploy the process.		
10.	BPM Solution should have the capability to define a custom algorithm for task routing based on custom attributes.		
11.	The task routing capability in BPM should support default algorithms like round robin, least busy, most efficient etc.		
12.	BPM platform shall support easy to use design interface (e.g. drag and drop of workflow components) for designing / modifying process models by authorized users over web browser		
13.	Tool should provide reusability for the connectors to systems/applications		
14.	Tool must provide abstraction of Process Definition from its Technical representation. A business user should be able to model the business process, separate from the technical aspects of the process. Specify levels of process, which can be modeled by business users in the modeler		
15.	Tool/IDE must support 64-bit.		
16.	Proposed solution should support Processes be designed / modified using a Web based modeler		
17.	Business process can be of Person-2-Person, Person-to-Application or Application-to-Application type. The proposed tools should have capability to model all these types of processes.		

SN	Features	Availability (Y/N)	Remarks
18.	Proposed solution should support tool supports modeling of sub-process with support of synchronous and asynchronous call		
19.	Proposed solution should provide an option of passing data from parent process to child process and returning of data from child process to parent process.		
20.	BPM platform should conform to industry workflow standards like BPEL, BPMN2.0. It shall provide a web interface should not require any proprietary software to be installed on client machines.		
21.	Proposed solution should provide the Modeler to be used to define error handling within the process. it should provide an option of defining compensating activities or option of modeling exception flow.		
22.	It should enable designers to visually construct services, data transformations, BPEL orchestrations and integration to applications and back-end systems.		
23.	Proposed solution should support rollback and compensating transactions/exception		
24.	Proposed solution should provide high reliability and support for long-lived processes that cross multiple applications by providing compensating transaction rollback and recovery.		
25.	Proposed solution should support modeling tool which has capability to execute the process end to end without deployment during development		
26.	Proposed solution should support modeling tool store Business Processes to a common centralized repository for managing process		

SN	Features	Availability (Y/N)	Remarks
	deployments throughout the runtime environments—essential for program-wide governance.		
27.	Proposed solution should support modeling tool for tagging (assigning of tags) of artifacts / process parameters.		
28.	Proposed solution should support modeling tool which have the capability to have model UI collections / UI templates / views.		
29.	Proposed solution should support capability to integrate with ECM systems at the Form / UI design level based on CMIS standard.		
	Proposed solution should support modelling tool support collaboration at design time i.e. multiple developers working on the same process at design time		
30.	Proposed solution should support the capability of versioning when the project is saved after changes.		
31.	The proposed modeling tool should provide a Process Server registry or equivalent with centralized tools to install and track deployed versions of multiple processes across various runtime server environments.		
32.	Web based modeling tool must be capable of handling Business Rules definition		
Execution			
33.	The proposed solution should have capability to process engine to send/receive asynchronous communication.		

SN	Features	Availability (Y/N)	Remarks
34.	Tools supports execution of sub-process with support of synchronous and asynchronous call.		
35.	The proposed solution should have tool to schedule future events, steps, sub processes and process executions		
System Integration			
36.	BPM engine support integration with applications (systems) in the enterprise participating in the process flow. Specify support for various application types and environments, e.g. Java., APIs		
37.	BPM platform should allow integration with standard portals and allow single sign-on.		
38.	BPM engine should allow integration with some mail clients e.g. SMTP protocols to send out mails for notification.		
Business Rules Feature			
39.	BPM engine allows integration with Rules engine.		
40.	The business rule should support all rules and policies relating to processes should be centralized at one place and should be reusable across multiple applications. The rules can be of type work Assignment or jurisdiction, delegation rules, process flow rules, computation rules, run time rules like vacation, delegation etc.		
41.	Rules should provide various styles of defining rules like • computation rules		

SN	Features	Availability (Y/N)	Remarks
	• work assignment rules • Delegation rules • Run time rules (vacation, delegation etc.) • Approval rules • Escalation matrix		
42.	Business rule must support complex Decision Tables type of rules for easy implementation of rules.		
43.	Business Rules must provide easy to use web-based editor for creating and editing rules. These tools must be part of the unified design-time environment		
Security			
44.	Solution should support the user authentication such as user-name/ password, One-time password before he/she can participate in process execution.		
45.	Solution should support tool be integrated with user repositories like LDAP.		
46.	Human Task		
47.	The proposed solution should handle human interaction with the process/BPM tool		
48.	The proposed solution should support intelligent routing capabilities. Tool support automatic routing of work to various participants		

SN	Features	Availability (Y/N)	Remarks
49.	The proposed solution should offer possibility of allocating one task to multiple users		
50.	The proposed solution should have ability to set the priority of the task		
51.	The proposed solution should have an ability to easily remove or route the task out of the queue - rules based automatic and manual reassignment.		
User Interface Development			
52.	The tool support development of user interface - forms using a WYSIWYG editor.		
53.	The proposed solution should support from control be integrated with external data source to pre-populate reference data		
54.	The UI forms be easily integrated with the workflow.		
55.	The UI support access-based control to display data to authorized people.		
56.	The BPM Web Portal should provide support for inline task completion i.e. Completion of tasks directly from the task list without opening the task.		
57.	It should support/include UI based visualization tools e.g. dashboards, graphs, easy models of processes and webforms.		
Process Monitoring - BAM			

SN	Features	Availability (Y/N)	Remarks
58.	The proposed solution should support out of box tools available for monitoring and analysis of business processes.		
59.	The tool has ability to measure of timelines of tasks		
60.	The tool should have capability of tracing Process instance End to End		
61.	The proposed solution should support real time monitoring of process by user, managers or administrators. Availability of dynamically changing, customizable dashboards		
62.	The proposed solution should support user define/configure parameters for which he/she can get reports		
63.	The proposed solution should support setting rules to respond to sets of events and pre-built KPIs		
64.	The proposed solution should support capability to business users to create adhoc reports dynamically based on some preset parameters		
65.	The proposed solution should provide reports that shows how many inflight tasks Broken down by status		
66.	The proposed solution should support tool have reports that shows Team member’s individual statistics		
67.	The proposed solution should have support tool to generate reports that show tasks assigned/status to a particular team member.		
Case Management Capabilities			

SN	Features	Availability (Y/N)	Remarks
68.	The proposed solution should support creation of Case activities for ad-hoc collaboration		
69.	The BPM platform should support the following ✓ Case Details instance viewer ✓ Case Folder / Document viewer ✓ Case Work Items viewers ✓ Case Search ✓ Case task visibility via Dashboards • case documents • case stakeholders • case milestones • case events		

7.4. Enterprise Monitoring System

The Monitoring system should be able to provide automated consolidated SLA reports for all the SLAs as mentioned in this RFP including real time status of various service levels achieved. The reports are to be available through a centralized web access / dash board, the access for this to be given to users as defined by IAAD.

The dash boards to be made for two levels (higher management level as well as operational dash board) for OIOS operations team.

SI will implement dedicated EMS solution to meet the SLA monitoring and other requirements as mentioned in the RFP. The implemented EMS solution is to help IAAD in data driven decision making. In case the SI uses any OEM product(s), the implementation should be as per best practices of the OEM.

The entire EMS implementation shall be certified by the SI also for its correctness, adequacy to meet RFP requirements and measurement of SLAs & KPIs etc. IAAD reserves the right to engage STQC/Other independent auditors for validating the deployment of EMS facilities as per RFP requirements, specially their capabilities for measuring and reporting SLAs & KPIs as defined in RFP. SI shall also provide in-depth training to the IAAD users (as per the SLA) on usage and operations of EMS solution.

SI has flexibility to offer EMS on PaaS model or perpetual license basis.

7.4.1. Server Monitoring

SN	Features	Availability (Y/N)	Remarks
1.	Should offer service driven operations management of the IT environment to manage distributed, heterogeneous systems - Windows, UNIX & LINUX from a single management station.		
2.	Should provide a centralized point of control with out-of-the-box policy-based management intelligence for easy deployment for the servers, operating systems, applications and services for correlating and managing all the IT infrastructure components of a business service		
3.	Should support Virtual platforms and provide capability to manage both Microsoft .NET and J2EE applications from the same platform		
4.	Should provide simplified service / process monitoring and have the capability for distributed management functions and should be accessible from any location.		
5.	Should provide in built correlation to reduce the number of messages presented to the operators and to determine the root cause.		
6.	The system must be agent based for managing the nodes and have the capability of storing events / data locally if communication to the		

SN	Features	Availability (Y/N)	Remarks
	management server is not possible due to some problem. This capability will help to avoid losing critical events.		
7.	EMS must support the backup server concept, which enables switching management responsibility from one management center to another in case of system failure. This eliminates single points of failure in the management system		
8.	The System Should have automated service discovery, policy deployment and actions to enable busy IT personnel to focus on more strategic initiatives and manage business-critical application services from the end-user perspective, and to be immediately aware of the business impact of lower level component failures or performance degradations		
9.	Complex dependencies between managed elements must be captured, allowing IT management staff to interpret lower level data in terms of its importance to the higher-level service.		
10.	An advanced real-time status propagation mechanism in the Services view must allow IT management staff to immediately determine the impact of a component failure on the overall application service. Problem-solving efforts can then be prioritized.		
11.	Alarms with meaningful message text, instruction text, operator / automatic actions / linked graphs, duplicate message suppression.		
12.	Should be configurable to suppress events at the agent or managed node level itself and be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.		

SN	Features	Availability (Y/N)	Remarks
13.	The system should allow for enriching of messages with incremental information and should allow for customization of message attributes.		
14.	There should be a single agent on the managed node that provides the system performance data, and for event management, it should be able to prioritize events, do correlation & duplicate suppression ability to buffer alarms and provide automatic actions with capability to add necessary annotations.		
15.	The system must support multiple built in discovery mechanisms for e.g.: Active Directory, Windows Browser, DNS with capability to discover and services discovery		
16.	The discovered services should be displayed in service dependency maps automatically for consolidating different IT management views into a single workbench, which ensures the health of end-to-end IT services across IT infrastructure and domains		
17.	Should provide console and a web browser interface that can be accessed from anywhere using industry-standard web browsers.		
18.	Each operator should be provided with user roles that should include operational service views enabling operators to quickly determine impact and root cause associated with events.		
19.	Highly scalable with ability push deployment of agents and monitoring policies to a variety of heterogeneous platforms enabling fast and controlled roll out and maintenance.		
20.	The agents should be extensible and customizable allowing incorporation of any required monitoring source not included in the out-of-the-box monitoring policies. With capabilities to collect and		

SN	Features	Availability (Y/N)	Remarks
	analyze performance data from the operating system and installed applications and use historical patterns to establish performance baselines.		
21.	Agents on the managed node should be autonomous and can undertake automated corrective actions in isolation from the Management server. This will provide management by exception for only forwarding actionable events to the Management server.		
22.	The system must include very powerful event management and correlation services technology, providing correlation capabilities on the agents in addition to the central manager station to filter, correlate, process, and respond to the thousands of events that are created daily from systems, databases, and applications.		
23.	There should be secured communication between Management server and Managed nodes avoiding the need to open unsecure firewall ports.		
24.	The system must provide a Manager-to-manager communication allowing management hierarchies to be established, such as several regional management centers linked to one central location, and to forward or escalate alerts depending on escalation rules. Escalation and forwarding must be fully automatic or handled through manual selection by Customer management staff.		
25.	The system may have its native database and capability to use external database like MS-SQL, Oracle etc.		
26.	The system should integrate with Helpdesk / Service desk tool for automated incident logging and also notify alerts or events via e-mail or SMS.		

SN	Features	Availability (Y/N)	Remarks
27.	The system should have management polices to monitor and manage WMI, Performance, SNMP, Application, Log Files and Event logs and support automatic action in various forms like running a script to be taken on alerts from managed nodes		
28.	The system should provide adequate help in capacity planning and provide trend analysis reports based on historical performance data		
29.	Centralized view for Agent-based and agent-less monitoring managed from one central console.		

7.4.2. Monitoring: OIOS Application Performance (Real User Monitoring, Diagnostics)

SN	Features	Availability (Y/N)	Remarks
1.	End to end Management of applications (J2EE/.NET based) with deep-dive diagnostics		
2.	Determination of the root cause of performance issues whether inside the Java / .Net application in connected back-end systems or at the network layer.		
3.	Automatic discovery and monitoring of the web application environment and ability to monitor applications with a dashboard.		
4.	Should have capability to monitor the third-party applications without any source code change requirements.		
5.	Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnose.		

SN	Features	Availability (Y/N)	Remarks
6.	Monitoring of application performance based on transaction type.		
7.	It should proactively recognize and isolate transaction performance bottlenecks in complex composite applications along with intelligent alerts based on user defined thresholds		
8.	It should deliver response time monitoring of both real-user and synthetic transactions		
9.	The system should offer a comprehensive end-to end transaction management solution for IT operations that may need to track transaction flows across heterogeneous environments.		
10.	Should drill down from slow, end-user transactions to the bottlenecked component, method or SQL statement, helping to solve memory, exception and other common problems		
11.	Should automatically detect all components touched by a business process across layers and traces them with no user intervention		
12.	Should display the detailed Application call-tree that pinpoints the exact slow method within method call stack		
13.	Should support J2EE, .NET based applications		
14.	The proposed solution should expose performance of individual SQL statements within problem transactions		
15.	Data, reports and views from the real user monitoring solution should be able to be incorporated into common dashboard views along with real user monitoring and infrastructure monitoring.		

SN	Features	Availability (Y/N)	Remarks
16.	The solution must be able to scale to reflect performance and availability from many geographical locations where business services are accessed without a significant increase in solution		
17.	Dashboards should be easily customizable using visual editing capabilities and no coding. They should be role-based so that business and IT stakeholders get the necessary visibility into the health of business and provide out-of-box KPIs that can be used to present different aspects of business service health.		
18.	Should be able to provide the breakdown of the time spent on each component across presentation, business and database layers.		

7.4.3. Database Monitoring System

SN	Features	Availability (Y/N)	Remarks
1.	The solution should monitor multiple database servers and multiple versions of each server including: Oracle/ SQL Server/ Informix/ DB2/ Sybase/ MySQL etc. including database proposed by SI.		
2.	The Solution should provide SQL Response Time for Monitoring Custom Queries.		
3.	Database Space Monitoring for both file group and transaction log (Warning threshold, Critical threshold as well as file group/ log full)		

SN	Features	Availability (Y/N)	Remarks
4.	Performance monitoring - capture of DB Engine related performance counters as well as threshold alerting		
5.	The solution must support SQL Agent monitoring - failed jobs, long running jobs.		
6.	The solution must be able to report & check for last recent Full database backup and last recent Transaction Log backup		
7.	The solution must monitor for Blocking (exceeding duration) and Deadlocks		
8.	The solution must be able to run power shell, vbscript, cmd and vbscripts to perform tests on the database and have the results put into the solution as performance data and or alarms.		
9.	Inclusion of SQL statements within the Solution should be a standard "easy-to-use" function achieved without programmatic intervention.		
10.	The solution should support auto - discovery of database instances.		
11.	The solution should support the use of schedules and time filters for database monitoring.		

7.4.4. Dashboard & Reporting (Events co-relation, Centralized Reporting)

SN	Features	Availability (Y/N)	Remarks
1.	The proposed Service Operations Management Dashboard must provide built in a manager of manager/MoM-class event management system for correlating cross-domain events, creating alerts based on		

SN	Features	Availability (Y/N)	Remarks
	correlated events and enforcing standardized escalation and automated action policies. The tool should support event correlation which uses rules and filters to identify commonly occurring events or combinations of events or need a new replacement event to be generated.		
2.	Proposed Dashboard solution should have Out-of-the-Box connectors/ probes to integrate with multiple EMS solutions, including industry standard solutions from HP, IBM, CA, Microsoft etc., and should also provide mechanisms (XML, APIs etc.) to integrate with other EMS and NMS solutions.		
3.	The solution should have cross-domain reporting module which allows to make future decisions by seeing behavior patterns by topology, service, application, operating system, virtualization platform/technology like hypervisor, middleware, database, etc.		
4.	The system should provide event Correlation Rules, meaning if there is rule relating a database problem to a file system problem, and another rule that relates a file system problem to a storage problem, the system should be able to link these rules together and link the database problem to the storage problem during execution time		
5.	When many a combination of many events occurs in the monitored environment, the system must be able to automatically categorize them into causes and symptoms. The system needs to provide a single interface to view multiple layers of cause and symptoms.		
6.	The system should support concepts of agent or agent less and it should provide ability of correlation rules, tools, and KPIs for specific managed domains such as J2EE, Database, and System Infrastructure.		

SN	Features	Availability (Y/N)	Remarks
7.	The system shall allow administrators to create new Event Correlation rules and indicating which event is the cause and which are the symptoms.		
8.	In case of server monitoring the adaptive threshold, capability is required on basis of previous trends in performance. Based on these trends, the threshold values are automatically and dynamically calculated. Once the automatic threshold values are set, comparing the current performance data with the adaptive thresholds indicates if the current infrastructure resource utilization is normal or not. An alert is generated when abnormal behavior is detected.		
9.	Tool should provide superior view of infrastructure health across system, networks, IT infrastructure and end-user into a consolidated, central console.		
10.	Should provide reports that can provide IT service quality levels, such as application response times and server resource consumption on the same pane.		
11.	Reports can be scheduled to publish automatically or they can be produced on demand.		
12.	Reports can be applied to all systems, to a group of systems, to a customer group of systems, or to a single system.		
13.	Reports can be published in HTML, PDF, Word, and Excel formats.		
14.	Should be possible to send reports via email from the Reporter GUI or from command line.		

SN	Features	Availability (Y/N)	Remarks
15.	Server reporting tool should be able to collect and collate specific information regarding the relationships between the IT elements and the business services.		
16.	Tool should be able to deliver comprehensive, long-term, and customizable cross-domain reporting.		
17.	Tool should provide a library of out-of-the-box reports that can be cross-launched in the context of business services.		
18.	Tool should provide the capability to prove the variety of reports using data sources such — Generic .csv files, and Databases supporting JDBC. Should also be included to pull data and create reports from such data.		
19.	Tool should allow to configure/ define change/ maintenance window for monitored infrastructure		

7.4.5. Service Desk (SLA monitoring, Incident Management)

SN	Features	Availability (Y/N)	Remarks
1.	The proposed solution shall provide a web-based service support system to automate incident, problem, change, knowledge management, interactive support, self-service and Asset management.		
2.	The proposed solution shall support tracking of SLA (service level agreements) for call requests within the service desk through service types (that define response/resolution time)		

SN	Features	Availability (Y/N)	Remarks
3.	The proposed solution shall provide appropriate standards-based integration mechanisms that allow infrastructure management solutions to automatically register incidents.		
4.	The proposed solution shall provide classification to differentiate the incident via multiple levels/tiers of categorization, priority levels, severity levels and impact levels.		
5.	The proposed solution shall provide the flexibility of automated incident assignment based on metrics such as analyst workload, category and location.		
6.	The proposed solution shall provide a web-based knowledge base that assists in finding, organizing, and publishing knowledge articles that aid in self-service & faster turn-around time.		
7.	Should support knowledge management best practices. Should provide out-of-the-box workflow.		
8.	The solution should provide ticketing where the user can take a screenshot of the error message and can attach to the service request. The user can type in a couple of text lines to describe the error in simple natural language. Rest of the details are picked by the service desk agent from the pictures/screenshots attached or the text description provided. The service desk agent then can pick up the ticket to provide the resolution of the same with the information already filled in (category, impact, and assignment).		
9.	When receiving a call from an end user, the user’s description of the issue can be entered as is by the help desk agent. Then, the agent should be capable to suggest the most likely categories and service for		

SN	Features	Availability (Y/N)	Remarks
	the help desk agent to choose. Any of the fields that were auto-generated can then be adjusted or corrected, if needed, also enabling the system to learn adaptively to be smarter in the future.		
10.	The proposed solution shall provide problem management module for recording problem work around and solution must be able to relate and link problem to specific incidents, knowledge management should provide service desk personal with speedy and accurate resolution to their problem either from Browser and ticket screen.		
11.	The solution should provide the capability to search previously saved service request, incidents, problems to help agent resolve the current issue at hand faster.		
12.	The solution should offer similar ticket search facility that should result only list service requests, incidents, and problems having the same Classification.		
13.	Should support end user chat where the end users can communicate with a Service Desk IT agent in real-time to quickly address the service requests and support requests as they arise.		
14.	The solution should provide the capability to integrate with mail server, so that the user can send the mail to the service desk, email is regarded as inbound email in the system. Based on the inbound email the service desk tool can create and update a record, and then the service desk agent will reply to the user with the suggested solution. When the service desk sends this email to the users it is regarded as an outbound email in the system. Both inbound and outbound emails should be reflected in the communication log as a part of the ticket record.		

SN	Features	Availability (Y/N)	Remarks
15.	The solution should provide personalized and role-based dashboards for all key IT processes where out of the box reports should be available covering all Service Manager modules.		
16.	The service desk users should be able to define their own reports via drag & drop functionality in seconds according to their business needs.		

7.4.6. OIOS, IT Infrastructure Operational Analytics (Log Correlation & Analysis)

SN	Features	Availability (Y/N)	Remarks
1.	The solution should allow for smart discovery which would run on a continuous basis and tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.		
2.	The NMS must allow immediately determining the impact of a component failure and thus helping in prioritizing problem-solving efforts.		
3.	The NMS should provide very powerful event correlation engine and thus must filter, correlate & process, the events that are created daily from network devices. It should assist in root cause determination and help prevent flooding of non-relevant console messages.		
4.	Polling intervals should be configurable on a need basis through a GUI tool, to ensure that key systems are monitored as frequently as necessary.		

SN	Features	Availability (Y/N)	Remarks
5.	The topology of the entire Network should be available in a single map along with a Network state poller with aggressive/customizable polling intervals		
6.	The NMS application should provide a Unified Fault, Availability and Performance function from a single station only to reduce network and device loads with unified fault & performance polling.		
7.	The NMS performance system must provide customizable reporting across the network domain.		
8.	The Network performance operator console should provide operators with seamless transitions from fault data to performance reports. For example - select a node in NMS fault mgmt. system and cross launch it for historical and near real time data.		
9.	Should have MIB browsing, MIB loading, and MIB expression collection features.		
10.	NMS should have support for SNMPv3 & IPv6, including dual-stack IPv4 & IPv6 to provide flexibility in protocol strategy and implementation.		
11.	Should enable efficient workflows using contextual navigation between reports and rich interactive report configuration capabilities		
12.	Data collection and thresholding of network device ports (any that support MIB2 including virtual interfaces): Bytes In, Bytes Out, Discards, Errors, Network Delay		
13.	Data collection and threshold setting of network devices: CPU, Memory, Buffers, Component statistics		

SN	Features	Availability (Y/N)	Remarks
14.	The proposed solution should provide various reports out of the box and should also provide the ability to create /generate customized reports.		
15.	Should honor network fault management tools' secure grouping and multi-tenancy settings		
16.	Should be able to schedule key reports for automated delivery		
17.	Distribute reports by email in HTML, Excel or pdf formats.		

7.4.7. End-User Experience Management System

SN	Features	Availability (Y/N)	Remarks
1.	The proposed solution should measure the end users' experiences based on transactions without the need to install agents on user desktops.		
2.	The solution should act as a passive listener on the network thus inducing zero overhead on the network and application layer.		
3.	The proposed system must be able to detect user impacting defects and anomalies and report them in real-time: • Slow Response Time • Fast Response time • Low Throughput • Partial Response		

SN	Features	Availability (Y/N)	Remarks
	• Missing component within transaction		
4.	The proposed system must be able to provide the ability to create user groups based on application criteria or location and link user IDs to user names and user groups.		
5.	The proposed system must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.		
6.	The proposed system must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web application.		
7.	The proposed system must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.		
8.	The proposed solution should be capable of identifying the problem domain (browser, network or application) thereby it should monitor the browser side metrics and provide reports in real time for: • DOM Construction Time (ms) • Page Load Time (ms) • Previous page unload time (ms) • Browser Render Time (ms) • Page Roundtrip Time (ms) • Responses Per Interval (browser activity)		

SN	Features	Availability (Y/N)	Remarks
9.	The proposed solution must be able to provide real time transaction health metrics and end user experience quality metrics anytime, anywhere for the business executives.		
10.	The proposed solution must be able to provide the IAAD Officials/ IT team the flexibility to select, organize and monitor real time business.		
11.	The proposed solution must be able to work consistently on a variety of mobile devices such as iOS, Android OS based etc.		
12.	The proposed solution must be able to provide flexibility by enabling addition of annotations to business indicators to enhance clarity and context around its behavior enabling better information sharing and collaboration.		

7.4.8. SLA Monitoring System

SN	Features	Availability (Y/N)	Remarks
1.	General: The solution most support Service Level Agreements Lifecycle Management including Version Control, Status Control, Effectively and audit Trail.		
2.	General: The solution must provide a flexible framework for collecting and managing service level templates including Service Definition, Service Level Metrics, Penalties and other performance indicators.		
3.	Service Delivery: The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective.		

SN	Features	Availability (Y/N)	Remarks
4.	Contract Management: The solution must support dependencies between supplier contracts and internal or external contracts.		
5.	Bonus & Penalty: Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs. Support for Defining and Calculating service Bonuses based on clauses in SLAs.		
6.	Alerts: The solution must support delivery mechanisms to indicate/notify whether SLA targets are being achieved or violated.		
7.	Business Impact Analysis: The solution must make it possible to find the underlying events that cause the service level contract to fail.		
8.	Dynamic Calculations: The solution supports dynamic service level targets to reflect obligations importance and priority over time.		
9.	Audit Trails: Full electronic audit trails available for both system and user transactions.		
10.	Reporting: Report module and SLA Management module must be integrated to provide ease-of reports configuration and execution.		

7.5. Reporting

SN	Features	Availability (Y/N)	Remarks
1.	It should support ad-hoc reporting with an easy to use self-help web launched interface.		

SN	Features	Availability (Y/N)	Remarks
2.	Solution should Flexible report layout.		
3.	Interactive report viewer should provide table and chart changes including sorting, filtering, conditional formatting, moving/hiding columns, string search, zoom in/out, along with format changes that can be saved for re-use.		
4.	Ability to present Data either textually or graphically		
5.	Developers can supply data in multiple ways and from Multiple data sources including remote data source.		
6.	Watermarks can also be applied		
7.	Ability to generate Sub reports		
8.	Ability to export Various common formats of reports		
9.	The solution should support key extensions such as DHTML, Excel, PDF, Word and Image rendering extensions; MHTML, CSV, XML, and Null rendering extensions		
10.	It should support Report caching, Report history; It should support Scheduling.		
11.	It should support Visualization tools.		
12.	The Solution should support drilling-down on data displayed in reports/dashboards to automatically show the detail comprising that data.		
13.	It should be able to create interactive scorecards and dashboards with an ability to drill down into details.		

SN	Features	Availability (Y/N)	Remarks
14.	The solution should support dynamic and interactive analytical charts and grids against which drill-to-detail, drill up/down, cross-drill, expand/collapse can be performed.		
15.	It should support user's access to generate, create, change and read the reports, and queries in the system. It should be defined and restricted based on each user's roles and responsibilities		
16.	It should support Automated and secure log and audit trail of reports run, reports accessed, and reports changed etc. E.g. User and Date and Time of change		
17.	The solution should support calculations/computations within reports		
18.	It should also support for maps and geospatial visualizations.		
19.	It should support/include UI based visualization tools e.g. dashboards, graphs.		
20.	It should provide a platform for advanced users to apply various (SQL) querying in the OIOS supported databases.		

7.6. Virtualization software

SN	Features	Availability (Y/N)	Remarks
1.	Should provide bare-metal architecture. Insert a robust virtualization layer directly on the server hardware.		

SN	Features	Availability (Y/N)	Remarks
2.	Should provide CPU virtualization. Run many operating systems and applications encapsulated inside virtual machines on a single physical server.		
3.	Virtualization software should support all offered Operating systems		
4.	Should provide resource management for virtual machines		
5.	I/O resource Management Should provide QoS /physical disk mapping capabilities for storage I/O.		
6.	The virtualization software should support for I/O or Compute node classification to optimize resource utilization without impacting production load.		
7.	Should have provision to add/increase virtual CPU, RAM & Disk to a running virtual machine without having to suspend/ shutdown/ restart the virtual machine.		
8.	Virtualization software should support live virtual machine migration.		
9.	Should support NIC teaming and redundancy.		
10.	Should provide network traffic-management controls to allow secure segregation of different types of traffic onto separate physical and logical channels.		
11.	Virtualization software should provide a mechanism to track VM resource utilization for capacity planning.		
12.	Virtualization software should embrace OSS with Enterprise support guarantee and remove vendor lock-in.		

SN	Features	Availability (Y/N)	Remarks
13.	Virtualization software shall include Enterprise supported openstack integration and management for vendor neutrality without extra cost		
14.	Virtualization software should be based on open-source hypervisor platform to support vendor agnosticism.		
15.	Virtualization platform should be certified to run the application workloads.		
16.	Virtualization software should provide Storage Integration for single console management of SAN infrastructure.		
17.	Virtualization software should provide support for templates and assemblies for rapid application deployment.		
18.	Virtualization software should have inbuilt intelligence engine to select best available server for VM deployment		
19.	The overall solution should optimize the license utilization of Enterprise applications viz. should support app. vendor certified hard-partitioning etc.		

7.7. Virtualization Management software

SN	Features	Availability (Y/N)	Remarks
1.	Should provide the virtual infrastructure management tool for managing the virtual servers		

SN	Features	Availability (Y/N)	Remarks
2.	Virtualization management software console shall provide a single view of all virtual machines, allow Monitoring of system availability and performance and automated notifications with email alerts		
3.	Virtualization management software should have integrated Physical Host and Virtual Machine performance monitoring including CPU, Memory, Disk, Network, Power, Storage Adapter, Storage Path, Cluster services, Virtual machine data stores		
4.	Role base access control in management console Ability to define different administrative roles in the management console with different administrative rights		
5.	Virtualization management software console shall provide reports for Performance and utilization of Virtual Machines. It shall co-exist and provide standards-based API to integrate with leading systems management vendors		
6.	Virtualization management software console shall provide the Manageability of the complete inventory of virtual machines, and physical servers with greater visibility into object relationships		
7.	Virtualization management software should allow to deploy and import Virtual machines, virtual appliances in Open Virtual Machine Format (OVF).		

7.8. Server Operating System

SN	Features	Availability (Y/N)	Remarks
1.	Operating system: Linux, Unix, Microsoft, Sun Solaris.		
2.	Offered OS should be Enterprise/ Data Center edition.		
3.	The product or upgraded version of the Product should have Product life cycle of minimum 10 years after OIOS phase-2 deployment. Further it should not have any end of life mode for technical support.		
4.	In case of Open source OS, the source code of the operating System should be freely available from the OEM.		
5.	The Enterprise grade Server operating system should support the essential network services like Directory Services (LDAP), DNS, DHCP, Radius, Web Server, Application server, Cluster services (High Availability and Fail over Support), Load Balancer, with virtualization support.		
6.	OS should conform to TCP/IP communications standards interface based on Internet Standards. The OS should support protocols / services / standards including, but not limited to, IPv4, IPv6, ICMP, IP Multicasting, User Datagram Protocol, SNMP, HTTP, SSL with FIPS certification, Domain Name Service, Telnet, SFTP, NFS, CIFS, SMB, Bootstrap Protocol, DHCP, Network Time Protocol, etc.		
7.	OS should have a robust architecture built for reliability and availability. The OS should support features including, Dynamic kernel patching without reboot.		

SN	Features	Availability (Y/N)	Remarks
8.	Support for I/O load balancing and multiple pathing for storage subsystem and networking.		
9.	OS should also support mandatory access control for file system, processes & users.		
10.	OS should support Reliability, Availability, and Serviceability (RAS) features: a. Physical memory hot add b. Advanced Error Reporting (AER) for PCIe devices c. CPU logical on-lining / off-lining		
11.	The software should provide support for running multiple instances of OS for Virtualized guest on same physical host		
12.	The software should have kernel level dynamic tracing hooks to monitor and tune system performance without any overhead		
13.	The operating system should have a mechanism to patch not only kernel but also user space binaries viz. glibc, openssl etc. without any downtime. Such a feature should not be dependent cost or complexity of OS clustering.		
14.	Operating system should have complete management tools for full lifecycle management of OS viz. Provisioning, Patching, monitoring with compliance dashboards and GUI based reporting engine.		
15.	The OEM should provide unlimited indemnification for all binaries supported and shipped in the operating system.		

SN	Features	Availability (Y/N)	Remarks
16.	Operating system should support kernel-based virtualization such as KVM, Docker and LXC		
17.	OEM shall provide 24X7 support over web and phone.		
18.	In case of Open source OS, OS Support should be Enterprise support.		

7.9. Database OIOS

SN	Features	Availability (Y/N)	Remarks
	General requirement		
1.	RDBMS software should function on 64-bit operating system platforms offered for OIOS like Linux, AIX, and Windows		
2.	Ability to handle large amount of data effectively		
3.	To have optimum utilization of resources like storage and memory database should support flexible page or block size setting.		
4.	Database solution should have advanced row compression technique that uses two levels of compression dictionaries (table-level and page/Row level) to improve compression ratios, particularly as data changes		

SN	Features	Availability (Y/N)	Remarks
5.	Database solution should provide temp table and index level compression with optimizer choosing the best algorithm.		
6.	To increase ability to meet SLAs database solution should have capability to prioritize access to hot data and It should be able to automatically move and balance the data between different storage groups. Above said capability should be available with all types of file systems.		
	Architecture and Reliability		
7.	RDBMS software provides connectivity using native connectivity, JDBC, ODBC and connectivity to various technologies like .NET, ASP, Java etc.,		
8.	To manage the SLAs better, Database solution should allow changing priority to prioritize short running transactions over long running transactions.		
9.	RDBMS should provide controls over who, when, where and how applications, data and databases should be accessed.		
10.	RDBMS should have the capability to balance the i/o across the available disk for the database.		
11.	RDBMS should support active-active clustering with objectives of scalability and high availability.		
12.	RDBMS can provide standard SQL Tool for accessing the database. The tool should be able to monitor, maintain and manage the database instance, objects, and packages		

SN	Features	Availability (Y/N)	Remarks
13.	RDBMS must have backup and recovery tool, which can support the online, incremental backup. The tool can facilitate the media recovery, partial recovery and full recovery.		
14.	RDBMS should have option for Automated/manual identification and tuning of high load SQL Statements. It provides details about dynamic tuning capability of the database depending on workload requirement, system resources etc.		
15.	RDBMS can have fault tolerance, parallel processing, linear scalability, mixed workload capabilities		
16.	RDBMS should have ability to service concurrent multiple read and write requests and it can handle deadlock situations.		
	Manageability		
17.	Database solution should have ability to allocate storage from pre-defined disk pools, as needed		
18.	Database solution should have an ability to self-tune its memory parameters dynamically when the executing workload changes		
19.	RDBMS performance manager should have capability to quickly identify potential problems and notify IT staff using email notification, SNMP integration and interactive dashboards.		
20.	RDBMS should utilize a powerful repository of historical performance metrics for problem prevention, trend analysis. Solution should also help to provide customizable reporting and growth planning		

SN	Features	Availability (Y/N)	Remarks
	Security and Audit		
21.	RDBMS ensures inter-dependency of user concurrency and data consistency. It provides lock mechanism and multi version read consistency for the transaction processing		
22.	RDBMS should provide functionality to restrict the access to database tables through the application only. It should restrict users or DBA or any privileged user accessing the operational information through SQL Language / Tools like Toad etc., using direct connection.		
23.	Database solution should support role-based security model		
24.	RDBMS should provide preventive controls on privileged user access to application data.		
25.	RDBMS should separate security functionality from application functionality and database administration functionality.		
26.	For the compliance reason, Database solution should provide visibility of data at some point in the past.		
27.	RDBMS should prevent privileged IT users such as DBAs and administrators from accessing and modifying sensitive data		
	Licensing Requirement		
28.	The OEM should provide patches, updates and upgrades		

7.10. Data Repository

The OIOS application includes a Data Repository for the data collected by the audit offices from outside sources. This data is, generally, obtained from other Government Departments i.e. outside OIOS Application in the form of database dump file.

In order to extract data from database dump file, (at least first) instances of most common RDBMs are needed to be installed on PaaS model. So, the latest version of following RDBMs instances need to be deployed as per BoM:

a) MySQL

b) PostgreSQL

c) MS SQL Server

d) DB2

e) Oracle

The primary user of above system shall be DBA, who shall migrate data from above RDBMS instance to OIOS RDBMS for subsequent analysis purpose.

It may be noted that in case any of the above RDBMS are offered for OIOS Application, its individual instance in this section would not be required.

The delivery of above component is expected to be in Phase-II.

7.11. Web Server

SN	Features	Availability (Y/N)	Remarks
1.	Should support integrated Web server solution with request queuing and caching		
2.	Should support load balancing		

SN	Features	Availability (Y/N)	Remarks
3.	Should have the ability to store web server configuration data in XML or plain text.		
4.	Should support web-based administration		
5.	Should Support for Web Distributed Authoring and Versioning and Web Folders		
6.	Should support integration with certificate services		
7.	Should Support for Web Distributed Authoring and Versioning and Web Folders.		
8.	Supports industry standard Authentication to LDAP, Kerberos, and RSA token authentication.		
9.	Should support integration with certificate services.		
10.	Should supports non-blocking and blocking handlers, traditional and asynchronous servlets, and JSR-356 web socket handlers.		

7.12. Application Server

SN	Features	Availability (Y/N)	Remarks
Architecture			
1.	Should be completely Java EE 7 Compliant – with Web and Full profile both		
2.	Should also support stand-alone mode with server management console		
3.	Application server should support third party integration of LDAP/AD		
4.	Application server should support third party integration of messaging infrastructures		
5.	Should support “No Single Point of Failure for AppServer components” architecture		
Standards			
6.	Java JSE 8		
7.	Java EE7		
8.	SCA / SDO programming model		
9.	WS-AT, WS-COORD, WS-BA		
10.	IP v6		
11.	XPATH		

SN	Features	Availability (Y/N)	Remarks
12.	XQUERY		
13.	XSLT		
14.	All Leading and Major Databases (as specified in Database specifications)		
LDAP integration			
15.	Should be built for Standards and Interoperability: Supports a wide range of Java EE and Web Services standards.		
Development			
16.	Integration of development platform with SVN and Trac (Bug Management/Issue Management)		
17.	Maven based build system for build, reporting and documentation of application		
18.	Good set of documents should be available for development		
19.	Development platform should provide choice of development frameworks as well as run-time platforms to suit various scenarios		
20.	Development platform should support open standards-based methodology and also comply to open architecture for better interoperability across/with ecosystems		
21.	Should allow developers to choose the programming models and frameworks		

SN	Features	Availability (Y/N)	Remarks
22.	Should support Industry standard web server		
23.	Out-of-the-box Clustering, Caching, Fail-Over & Load Balancing support.		
24.	Discovery and management of cluster nodes		
25.	Failover and load balancing for JNDI, RMI, and all EJB types		
26.	Stateful session bean state replication		
27.	HTTP session replication		
28.	High-availability and JMS Clustering Support		
29.	Data Source failover		
30.	Dynamic Application Update without downtime		
31.	Test and rollout of new versions of application with no downtime		
32.	Should provide high availability for singleton services		
33.	Should support Transaction recovery during AppServer failover		
Installation			
34.	There should be a standard graphical installer.		
35.	It should be possible to fully automate the text-based installer with a 'response file' containing user-supplied configuration information.		

SN	Features	Availability (Y/N)	Remarks
36.	Should support standard text-based installer		
37.	There should be a production profile which starts typical production services with typical production settings, to Minimize the amount of post-install configuration.		
38.	Installation procedure for various deployment architecture should be well documented		
39.	Should be able to install web application binaries on a remote server from the web console		
Monitoring and Administration			
40.	Should provide RASP (reliability, availability, scalability and performance) combined with easy manageability features		
41.	Should provide easy to use wizards in the Web console to configure of the AppServer without requiring to manually edit the configuration files		
42.	Should not require a database to store the AppServer configuration		
43.	Should come with simplified, integrated, centralized administration, management tool.		
44.	It shall provide Diagnostic tools help isolate the source of problems		
45.	There should be a unified configuration & management		
46.	All administrative operations should be accessible via remote,		

SN	Features	Availability (Y/N)	Remarks
	secure Web-based User Interface secure Command Line Interface (CLI) secure programmable API		
47.	The management console should support multiple administrative users with discrete access control rights		
48.	Deploy multiple versions of the same application		
49.	Ability to transform UI operations into CLI commands		
50.	Centralized backup/restore of entire distributed topology		
51.	Server upgrade tool to preserve applications and configuration		
52.	Centralized installation of server patches and upgrades		
Operations and Management			
53.	Should provide support for side-by-side/production redeployment. So newer versions of application be deployed side-by-side with older version in same JVM		
54.	Should be able to deploy applications in multiple application server on a single click		
55.	Scripting of Administrative task should be possible		
56.	Server management should have performance and diagnostic viewer		

SN	Features	Availability (Y/N)	Remarks
57.	Should be able to raise unlimited production as well as development support tickets for timely resolution		
58.	Consistent and powerful management should be available out of the box		
59.	Should support backup and restore of the server's configuration repository		
60.	It should be possible to apply patches to an instance and those patches would be staged until the instance (re)starts at which point they will be effective.		
61.	It should be possible to roll-back the last batch of patches – restoring the instance to its previous state on (re)start.		
62.	All log messages should have a common log format and common categories.		
63.	Components of the server should support controlled shutdown or quiescence		
64.	It should be possible to manage the JVM configuration – i.e. JVM parameters		
65.	Administrative operations should typically be atomic – i.e. Have a predictable outcome – success or failure. Failure should typically result in the system reverting back to the original state		
66.	The administrative infrastructure should support "compound operations" so admin. Agents can invoke operations across groups or		

SN	Features	Availability (Y/N)	Remarks
	clusters of instances rather than enumerating through individual instances		
67.	By design goal: configuration changes should be dynamic – i.e. Take immediate effect and not require a restart. Exceptions should be clearly documented and the administrative UI's should make it clear that a restart is required		
68.	All components of Application Server should be configurable through the administrative Infrastructure		
69.	The CLI should allow for remote invocation.		
70.	The CLI should use the same authentications mechanism(s) as the Admin GUI.		
71.	All administrative operations for a single domain should be accessible via a remote, secure programable API		
72.	Validation of configuration changes should be performed at a number of levels – at the command line, the GUI the API and as an implicit validation command from any administration agent.		
73.	Proposed Application Server should be certified on leading JVM's, Operating System		
74.	Ability to remove a node for maintenance from a web console		
75.	Ability to add a node to the cluster without requiring a downtime		
76.	Ability to include a node for Approver request processing automatically		

SN	Features	Availability (Y/N)	Remarks
Security			
77.	For Administrative Security – it should be possible to integrate with and make use of existing infrastructure; e.g. need to connect to existing corporate LDAP.		
78.	Shall provide security infrastructure and mechanisms to protect sensitive Java EE resources and administrative resources.		
79.	Shall address enterprise end-to-end security requirements on authentication, resource access control, data integrity, confidentiality, privacy, and secure interoperability.		
80.	Capability to have separate administrative roles and limit scope of actions (super user, monitor, configurator, operator)		
81.	SSL shall be supported		
82.	All modifications through the administrative infrastructure should be audited		
83.	All administrative operations will be logged in order to provide an Auditable record of changes made to a domain configuration		
84.	Role-based Administrative security (who can do what)		
85.	Fine-grained administrative security (who can manage what)		
86.	LDAP support and compatibility		
87.	Kerberos support		

SN	Features	Availability (Y/N)	Remarks
88.	Authentication against ordered list of LDAP servers		
89.	Keys and Certificate Management		
90.	Multiple Security Configurations		
91.	Audit and track changes made to the server configuration		
92.	The product provides security infrastructure and mechanisms to protect sensitive Java EE resources and administrative resources and to address enterprise end-to-end security requirements on authentication, resource access control, data integrity, confidentiality, privacy, and secure interoperability.		
Scalability			
93.	Vertical scalability (on SMP machines)		
94.	Horizontal scalability (across clusters and non-cluster of machines)		
95.	The web server connector should support dynamic addition of Application Server nodes		
96.	Cluster wide JNDI naming service		
97.	Web caching (static HTML, servlet, JSP, full page, URL-based, file type-based)		
98.	Thread pooling, connection pooling, customized pools		

SN	Features	Availability (Y/N)	Remarks
99.	Ability to distribute HTTP client requests across multiple web containers		
100.	Ability to distribute RMI-IIOP client requests across multiple EJB servers		
101.	Ability to distribute JMS client requests across multiple JMS servers		
102.	Ability to manage extra-large configurations		
103.	Prioritization and throttling of the HTTP, JMS, IIOP requests		
Performance			
104.	Dynamic page fragment cache (Servlets, JSP, etc.)		
105.	SOAP-HTTP request caching		
Problem Isolation and Determination Tools			
106.	2 phase commit (XA) automatic transaction recovery after failures		
Performance tuning advisor			

7.13. KMS Platform, discussion forum

SN	Features	Availability (Y/N)	Remarks
Knowledge Management			
1.	Integration: KMS solution must integrate seamlessly with OIOS: Application, SSO, DMS, CMS, RDBMs, Workflow engine.		
2.	Ability to create multiple administrator for multiple Audit streams. These Administrators shall manage static content in their respective are of responsibility.		
3.	Ability to add/edit/update content or articles on a subject, specific solutions to an issue or question		
4.	Ability to search for content using simple keywords, document type, date range, etc. and share internally or externally as needed		
5.	Advanced search with combination (and/or) of multiple words with other options. Search results prioritized based on hit with metadata/subject (high) and content (low).		
6.	Ability to manage content creation including approvals		
7.	Ability to aggregate content from internal and external sources		
8.	Ability to create Taxonomy for content classification		
9.	Ability to set Accessibility/access permissions for Internal/ external users, for an Audit stream, individuals.		
10.	Ability to share Knowledge Articles externally if needed		

SN	Features	Availability (Y/N)	Remarks
11.	Ability to track content utilization and effectiveness		
12.	Ability to link with OIOS Application and access MIS Reports, data as required.		
13.	Ability for a user to save searches or content / information for quick access		
14.	Integrates with other OIOS solution components using Open API		
15.	Ability to Views/dashboards/reports pertaining to effectiveness of KMS platform and its content.		
16.	Accessibility: multi-device (Laptop, Tablet, Smart phone) online/offline access		
Discussion forum			
17.	Discussion forum component could be a separate solution or part of KMS. If it's separate component then should integrate seamlessly with KMS.		
18.	Discussion forum available accessible to only IA&AD users.		
19.	Accessibility: multi-device (Laptop, Tablet, Smart phone) online/offline access		
20.	Ability to create a group and add members		
21.	Ability to create/ view easy to use Forum Menu and Directory, sub forum		
22.	Topic functionalities:		

SN	Features	Availability (Y/N)	Remarks
	a. Template b. New Topic c. Mark/ Unmark as Topic d. Classify a Topic e. Locked Topics, Forums and Sub-Forums f. Locked Topic Reply Removal g. Topic Status Indicators h. Topic Summary		
23.	Search functionalities: a. Search, Sort and Filter b. Clear Search		
24.	Ability to identify and display Top contributors		
25.	Ability to rate a topic, contributions		
26.	Segmentation: Segmentation forum software shall show users the forums that are relevant to them.		
27.	User should be able to select Sub forum, Topic in which they are interested or relevant to them.		
28.	Intimation to user on email, when a new content from sub forum/ topic of their interest, response to their query is generated		
29.	email dispatch functionality for sending notification on email to users could be built in platform/ add on component		

SN	Features	Availability (Y/N)	Remarks
30.	Analytics Ability to collate data and reporting pertaining to discussions. This ranges from users' profiles to discussion activity to sentiment analysis.		
31.	**Favorites:** Users should be able to indicate which topics and discussions are relevant to them. Users can receive email alerts when a new post or comment is added in a certain area. Alerts-type features to be notified when a certain word or phrase is added to a discussion. "Favorites" features shall allow users to subscribe to a specific thread in a forum so that they can pinpoint and stay connected to exactly the conversations that are important to them.		
32.	Auto-Subscriptions Discussion specific to an audit stream, to which an Audit professional is part of, all users should automatically subscribe to.		
33.	Prompt display on Home page for: Important, popular discussions.		
34.	Terms of Use Ability to set up terms of use and include a link to it in each automated email message, as well as prominent places on the web site.		
35.	Preferred functionality Though not mandatory however notifications to each user in his/ her OIOS Dashboard functionality preferably be provided		

7.14. Helpdesk OIOS

Helpdesk Application for OIOS is required on subscription model. Its function shall be limited to ticketing of issues, its resolution, and summary of standards reports. SI need to propose a suitable solution.

SN	Features	Availability (Y/N)	Remarks
1.	Support channels shall include: phone, email, self-service.		
2.	Ticketing management to record and organize users' complaints into tickets and tracks their progress up from receipt to resolution.		
3.	Helpdesk solution shall be integrated with SLA monitoring tool for automatic generation of SLA data.		
4.	Knowledge access. This pertains to both internal and external users. Agents should be able to quickly retrieve product information to assist customers. Likewise, customers with repetitive questions should be directed to a knowledge base of FAQs so agents are free to focus on unique tickets.		
5.	Solution shows the ticket status to users.		
6.	Ability to avoid duplicating the ticket response for helpdesk agents.		
7.	Ticketing should also be able to convert emails to tickets relatively quickly (with a few clicks)		
8.	Functionality to have a knowledge base or self-service. It's one of the most important features of help desk software. It compiles customer questions and structures them into retrievable FAQs or how-to articles.		
9.	Repetitive queries can be directed to above section, freeing up helpdesk agents to focus on more urgent issues and at the same time		

SN	Features	Availability (Y/N)	Remarks
	allowing to provide 24/7 help desk since the knowledge base is always up		
10.	Escalation: escalation features where agents can route business related query to IA&AD and difficult tickets to the higher-ups. A good escalation allows for Multi-level submission where supervisors get to resolve issues within their authority instead of escalating the ticket further up.		
11.	Preferred feature: The software automates repetitive, predictable, or routine tasks including recurring customer questions and administrative tasks like filling up forms or issuing daily reports. Automation can span the entire range of support service from converting emails to tickets to routing them to the right agents. It also takes care of notifying managers of pending or resolved tickets.		
12.	Dashboards: a. agents see the most important data upon logging in. This may include pending, urgent and new tickets. b. should also show supervisors and managers key metrics like overall agent performance, resolution rate, and the number of issues resolved per week or month.		
13.	**Analytics**. Ability to organize queries in visual ways that reveal valuable information like top product complaints, demographics, etc.		
14.	Time tracking to measure the resolution rate per agent		

SN	Features	Availability (Y/N)	Remarks
15.	**Email compatibility.** Help desk software be compatible with IA&AD email client.		

Note: In case offered EMS Tool provides all the Helpdesk functionalities stated above, then Helpdesk can be offered as part of EMS. The SI should explicitly mention this in his bid.

7.15. Site Recovery Software

SN	Features	Availability (Y/N)	Remarks
1.	Should monitor both Data Centers for its availability		
2.	Should provide automatic/manual trigger to start services at DR site (Data Center -2/ as applicable).		
3.	Site recovery software console shall provide a single view of all the Data Centers		
4.	In case of disaster at a Data Center, site recovery software should initiate following action but not limited to at DR site: a) Starting corresponding VM for a service b) Loading corresponding operating system c) Amending required network/ DNS configuration d) Loading corresponding application/ web server e) Loading corresponding database server, etc. f) All actions should be completed within stipulated RTO		

SN	Features	Availability (Y/N)	Remarks
5.	Site recovery software shall provide features to revert the services to parent Data Center as and when it is available.		
6.	Site recovery software shall provide reports for Performance and migration activities.		

7.16. Patch management

SN	Features	Availability (Y/N)	Remarks
1.	Should detect, collect and maintain information about Managed Servers, including packaged, unpackaged software, runtime state, host/guest relationships and more.		
2.	Should have`` capability to auto install agent onto target server		
3.	Bidders should provide patch management service to the offered Operating system and for the existing OS like Linux.		
4.	Identifies server missing patches quickly and easily and reduces the time needed to patch multiple servers. Enables patch policy creation and flexible patch deployments.		
5.	Enables rapid trouble shooting and patch management reporting to verify which are the client/ servers have specific patches installed / updates as per OEM best practices		
6.	Enables code and application deployment on servers in single or multiple instances without proprietary packaging. Imports files,		

SN	Features	Availability (Y/N)	Remarks
	objects, and scripts to define configuration best practices with graphical user interface (GUI) ordering or deployment and uninstall. Uses a granular permissions model to share applications with developers and administrators.		
7.	Uses the communications channel with enhanced security features, audit logs, to provide direct connections to servers in any location.		
8.	Improves automation efficiency by managing remote systems and executing tasks from a command line interface.		
9.	Provides reports into hardware, software, patches, and operations activities in complex, heterogeneous Data Centers. Includes out-of-the-box compliance reports and at a- glance compliance status with actionable links to servers, policies, and other objects. Exports reports to HTML and comma-separated values (CSV) formats.		
10.	The system should support automation of servers across multiple Data Center, with overlapping IP addresses, create and manage policies in any location and apply them to the entire environment.		
11.	The audit trails should be stored centrally		
12.	Will support automated enforcement of policies through fully automated check and remediation process		
13.	Will support audit and remediation against industry best practice content.		
14.	Tool should provide a powerful yet flexible solution that lets admin capture and leverage a shared application and deployment model. Users can enter information such as configurations and settings once		

SN	Features	Availability (Y/N)	Remarks
	which can be used each time the application enters that phase of the lifecycle which helps speed the deployment cycle.		
15.	The system should enable admin to manage any server from any facility (in other words, admin should not have to login to separate management consoles to manage servers in remote facilities).		
16.	System should provide a shell interface to let users operate through a command line across multiple servers simultaneously.		
17.	Scalability – a single instance should be capable of managing the entire lifecycle of servers for at least 100 servers		

7.17. Back Up Solution

SN	Features	Availability (Y/N)	Remarks
1.	De-duplicated backup and recovery – appliance/ solution based		
2.	Automation of backup efforts as much as possible		
3.	Maintain backup logs		
4.	Should support various level of backups including full, incremental, differential, as required by proposed solution		

5.	The software should support virtual platform offered for proposed solution		
6.	The proposed solution should have feature for alerting and reporting with pre-configured and customizable formats		
7.	Bidder should provide appropriate licenses for online backup agents and clients as per the RFP requirement.		

7.18. Geographic Information System

GIS application with minimal functionalities shall be provided on PaaS subscription model. SI needs to provision for Development/deployment licenses, if required.

SN	Features	Availability (Y/N)	Remarks
1.	User Interface to be simple and easy to understand and use.		
2.	Software to provide good graphical interface for the user, to operate on the system, performing the required task such as viewing the details of the Audit sites, and to allow user to view quick reports for selected site, session, office etc.		
3.	Software to provide a single module capable of performing Multi-layer spatial query on top of CAG datasets. A user should be able to save a query in his/her own session based on the credentials on the web client itself.		
4.	The user would be able to pass the query output directly into a dashboard scenario, wherein the user must be able to design a dashboard as per the user's requirements using the query output. The dashboard one created should be able to be saved as a local pdf file.		

SN	Features	Availability (Y/N)	Remarks
5.	The product should consume data directly from offered OIOS RDBMs with PostGIS without any bridge or middleware directly from native tables.		
6.	The GIS server software should Deliver data to OGC-compliant web applications. The software should facilitate interoperable web service interfaces for data, including OGC/ISO WMS, WMTS, WCS, WFS, and WFS-T with GML, KML, Geo RSS, and SLD support		
7.	The solution should catalog geospatial information by harvesting metadata and persist it in a central, searchable catalog. Simple harvesting from storage with thousands of datasets with footprints & thumbnails.		
8.	The software should have feature sets up listeners on directories to automatically crawl incoming raster, vector and multimedia files. It should automatically crawl the incoming data.		
9.	The software should Aggregate disparate data stores into homogenous layers with out-of- the-box hierarchical data models rendering through the OGC Web Map Service (WMS) interface, with Styled Layer Descriptor (SLD) support		
10.	The Software should provide Leverage extremely fine-grained security model to assign access, scale and spatial security permissions to every aggregate/dataset in the system per user/role. Should support full SSL		
11.	Should support LDAP and Single Sign-On.		
12.	Software should have logging information can be recorded for security or auditing purposes.		

SN	Features	Availability (Y/N)	Remarks
13.	Should have “On-The-Fly Re-projection” and “On-The-Fly Mosaic” functionalities.		
14.	Portal should have capability to map boundary and locations with exact latitude and longitude.		
15.	The GIS Web browser client must be able to interactively add data services on the fly on the client side by defining and maintaining data sources (few indicative examples as follows): a. Bing Maps b. Google Maps c. Open Street Map d. Bhuvan OGC etc.		
16.	The Web client must support scale-based printing interface wherein the user must be able to specify the following parameters: a. Page size (A3, A4) b. Orientation c. Scale d. DPI Settings		
17.	The Web GIS Server should automatically crawl, catalogue, and publish the Geotagged photos having spatial information from a storage or from database table. It should also allow it search/discovery by the using web client application based on user defined queries like location, timestamp etc.		

Note: Map updating need to be for Government offices/ Institutions up to Gram Panchayat, Village level.

7.19. Data Centre Hardware

7.19.1. Blade Chassis

SN	Features	Availability (Y/N)	Remarks
1.	Solution to house the required number of blade servers in smallest number of enclosures. Industry standard suitable for housing in Standard Server Racks.		
2.	Should support Hot Pluggable & Redundant Management Modules with on board/virtual KVM functionality.		
3.	Should provide a highly reliable and high-performance mid-plane/back-plane design in the blade enclosure. Should provide detailed technical information.		
4.	Should be able to accommodate the blade servers of specifications mentioned in the proposed blade enclosures. The proposals must offer the most dense packaging possible for the blade servers in the enclosure		
Interconnect			
5.	Support simultaneous remote access for different servers in the enclosure.		
6.	Should support simultaneous housing of FCoE /Ethernet/ FC/ SAS/ InfiniBand interconnect fabrics offering Hot Pluggable & Redundancy as a feature		
7.	Blade Server Interconnect to: LAN/ Network/ converged		

SN	Features	Availability (Y/N)	Remarks
8.	The enclosure should support redundant network / converged module / with at least 4 10G uplink ports, up-linkable to the Data Center switch		
9.	Blade Server Interconnect to Fiber Channel SAN/ converged		
10.	The enclosure should support redundant Fiber Channel SAN/ converged module with at least four nos 16 Gb auto-negotiating FC uplinks and also at least 16Gb auto negotiating downlinks to all server bays.		
Power Supply			
11.	The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should support N+N as well as N+1 redundancy configuration, where N is greater than 1. Should offer a single-phase power subsystem enabled with technologies for lower power consumption and offering high energy efficiency levels. Vendors should provide documents certifying the claims.		
Cooling			
12.	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics.		
Warranty			
13.	5 years comprehensive warranty.		
System Software			

SN	Features	Availability (Y/N)	Remarks
14.	Management/controlling software have to be from the OEM.		
Remote Management			
15.	Must provide a remote management functionality to operate the server in in-band/ out-of-band. Must be part of the server without the need to install any additional hardware or software.		
16.	Must have a real time Virtual KVM functionality and be able to perform a remote Power sequence. Must provide web browsing options.		
17.	Must have the ability to map the remote media to the server and ability to transfer files from the user's desktop/laptop folders to the remote server with only the network connectivity.		
18.	Must have the ability to capture the video/log sequence of the last failure and the boot sequence and also playback the video capture/log sequence or equivalent technology.		
19.	Must have the ability for multiple administrators across remote locations to collaborate on the remote session in a server with multiple sessions.		
Power Management			
20.	Must be able to show the actual power usage and actual thermal measurement data of the servers.		
21.	Vendors must submit supporting documents stating RoHS compliance.		

7.19.2. Blade Server

SN	Features	Availability (Y/N)	Remarks
	The OEM should fall in the Gartner's magic quadrant for Blade Servers.		
CPU			
1.	Two numbers of latest generation Intel 16 Core or higher. The processor should be one quarter in production at the time of supply		
Memory			
2.	128 GB RAM total scalable to at least up to 1TB, using DDR4 Load Reduced DIMM (LRDIMM) memory modules.		
Memory Protection			
3.	Advanced ECC with multi-bit error protection and memory online spare mode/memory mirroring.		
Hard disk drive with carrier			
4.	2 * 600 GB hot plug SFF SAS drives.		
Storage Controller			
5.	Integrated PCIe 3.0 based 12G SAS Raid Controller with RAID 0, 1 with 1GB of Flash backed write cache on board.		
Networking features			
6.	Dual 10 Gbps Ethernet ports/FCOE		
Interfaces			
7.	Minimum of 1 * internal USB 3.0 port and 1* internal SDHC card slot		

SN	Features	Availability (Y/N)	Remarks
8.	Should have 2x16 Gbps for FC/FCOE		
Bus Slots			
9.	Minimum of 2Nos of cards supporting Converged/ Ethernet/ FC adapters/ SAS/ IB adaptors		
Embedded system management			
10.	Blade should have manageability through blade / chassis management solutions with all features enabled highest enterprise license available. Solution should support virtual media.		
Security			
11.	Power-on password Administrator’s password Keyboard password (Quick Lock) Out of band/ in band remote management Chipset with • SSL encryption • Secure Shell version 2 • Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) On browser, CLP and XML scripting interface • External USB port enable/disable Network server mode Serial interface control TPM (Trusted Platform Module) 1.2 option		

SN	Features	Availability (Y/N)	Remarks
	Advanced Encryption Standard (AES) Intel® Advanced Encryption Standard-New Instructions (AES-NI) FIPS 140-2 Level-2 certification		
OS Support			
12.	All offered OS for OIOS		
Warranty			
13.	Server Warranty includes 5-Year Parts, 5-Year Labor, 5-Year Onsite support with next business day response		
Remote Management			
14.	a) System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB. b) Server should support agentless management using the out-of-band remote management port. c) The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur.		
15.	The Systems Management software should provide Role-based security		
16.	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.		

7.19.3. KVM Switch

S. No.	Features	Availability (Yes/No)	Remarks
1.	Rack mountable, 16 port or higher Analog USB KVM Switch.		
2.	KVM switch needs to be fitted in the rack itself.		
3.	All necessary cables to connect the servers to the monitor/keyboard/mouse must be provided by the bidder.		
4.	Warranty - 5 years comprehensive onsite OEM warranty		

7.19.4. SAN storage 40 TB

S. No.	Features	Availability (Yes/No)	Remarks
1.	The OEM should fall in the Gartner's magic quadrant for General purpose Disk Array		
2.	Offered Storage array shall be a true converge / unified storage with a single Microcode / operating system instead of running different Microcode / Operating system / Controllers for File, block. Offered Storage array shall be end-to end 12Gbps enabled which means that both Front-end Fiber channel ports and Back-end engines shall be operated at minimum 12Gbps speed.		
3.	The storage array should support offered OS.		

S. No.	Features	Availability (Yes/No)	Remarks
4.	Storage Array shall be offered with 40 TB usable capacity in RAID 5: • Storage should be scalable up to 60 TB usable in future using same or higher drive configuration • Distribution of Disk type is as follows: **a.** 20 % SSD **b.** 80% SAS		
5.	• Offered Storage Array shall be given with minimum of 64GB cache which shall be used only for Data and Control information. OS overhead shall not be done inside cache. • Offered Storage array shall also have additional support for Flash Cache/equivalent using SSD / Flash drives. Both File services as well as Block operations shall be able to utilize flash cache/equivalent. Minimum of 1TB Flash cache/equivalent shall be supported. • If Flash cache/equivalent is not supported inside the storage array then vendor shall ensure that offered storage array shall be scalable to minimum of 256GB DRAM cache without any replacement or upgrade of controllers		
6.	The offered storage should have enough compute power to perform all background activities optimally		
7.	Controllers shall be true active-active with no single point of failure while supporting all the major functionalities like Thin Provisioning, Data tiering etc.		

S. No.	Features	Availability (Yes/No)	Remarks
8.	Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc.		
9.	Offered Storage Array shall support dual-ported 300 / 600 / 1200 /1800GB hot pluggable Enterprise SAS hard drives, minimum of 400GB SSD Drives along with near line SAS 2TB / 4TB / 6TB drives.		
10.	Offered Storage Subsystem shall support Raid 1+0, 5 and Raid 6.		
11.	In case of Power failure, Storage array shall have de-stage feature to avoid any data loss.		
12.	Offered Storage array shall support all well-known protocols like FC ISCSI/ FCOE, SMB 3.0, NFS V4, NDMP etc.		
13.	Offered Storage shall have minimum of 4 host ports for connectivity to servers running at 16Gbps speed. Offered Storage shall also support: a) Additional Quad number of 10Gbps ISCSI / FCOE ports. b) Along with ISCSI / FCOE ports, additional Quad number of 10Gbps IP ports or eight numbers of 1Gbps IP ports if needed for File services operations. c) Offered storage shall have two additional IP ports for the storage-based replication. d) Offered storage shall have mum of 16 SAS lanes running at 12Gbps speed		

S. No.	Features	Availability (Yes/No)	Remarks
14.	1. Offered Storage Array shall support Global hot Spare for offered Disk drives. 2. Global hot spare shall be configured as per industry practice.		
15.	Shall have capability to use more than 30 drives per array group or raid group for better performance. Storage shall be provided with Performance Management Software. Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array. It shall be possible to change the quality of service of a volume for critical and non-critical workloads		
16.	1. Offered storage array shall be supplied with Thin provisioning and Thin Re-claim to make the volume thin for an extended period of time for complete array supported raw capacity. 2. Thin Re-claim (Zero Page reclaim) inside storage subsystem shall be automatic in nature and there shall be no need to run any utility inside storage for same. 3. Thin Re-claim inside storage shall not cause any overloading of Storage CPU and shall be able to claim the Zero pages even during peak load without any performance impact		
17.	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.		
18.	1. Offered Storage shall have support to make the snapshot and full copy (Clone).		

S. No.	Features	Availability (Yes/No)	Remarks
	2. The storage array should have support for both controller-based as well as file system-based snapshots functionality (At-least 256 copies for a given volume or a file store).		
19.	1. For file services operations, offered storage shall support both user level as well as file level hard and soft quota. 2. For file services operations, offered storage shall support integration with industry leading antivirus vendors like Symantec and MacAfee.		
20.	1. Vendor shall provide Storage Array configuration and Management software. 2. Software shall be able to manage more than one array of same family.		
21.	1. Offered storage shall support dynamic migration of Volume from one Raid set to another set while keeping the application online. 2. For effective data tiering, Storage subsystem shall support automatically Policy based Sub-Lun Data Migration from one Set of drive Tier to another set of drive tier.		
22.	1. The storage array should support hardware-based data replication at the array controller level across all models of the offered family. 2. The Storage array shall also support three ways (3 Data Centers) replication with or without using any additional replication appliance (Has to be provided as per the solution).		

S. No.	Features	Availability (Yes/No)	Remarks
	3. Replication shall support incremental replication after resumption from Link Failure or failback situations.		

7.19.5. SAN Storage 10 TB

S. No.	Features	Availability (Yes/No)	Remarks
1.	The OEM should fall in the Gartner's magic quadrant for General purpose Disk Array.		
2.	The storage array should support offered OS. Offered Storage Shall support all above operating systems in Clustering.		
3.	a. The Storage Array shall be offered with 10 Tb Usable Capacity Using 20% SSD, 80% SAS on RAID 5. b. For effective power saving, Storage subsystem shall be supplied with 2.5" Small form factor SFF drives however storage subsystem shall also support LFF drives with the addition of required disk enclosures. c. Storage shall be scalable up to 20 TB in similar offered configuration		
4.	a. Offered Storage system shall be supplied with minimum of Dual 16Gbps FC ports and Dual 10Gbps ISCSI ports per controller. b. Offered storage shall have flexibility to use all above ports either as FC or ISCSI by replacing the requisite SFP. Vendors shall provide the additional SFP accordingly. In case, vendor doesn’t		

S. No.	Features	Availability (Yes/No)	Remarks
	support this feature, then every controller shall be populated upfront with 4 x 16Gbps FC ports and 4 x 10Gbps ISCSI ports.		
5.	Offered Storage subsystem back-end engine shall be running on latest SAS (6Gbps) loop speed.		
6.	The storage array should support dual, redundant, hot-pluggable, active-active array controllers for high performance and reliability		
7.	Offered Storage Array shall be configurable in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc.		
8.	1. For SFF drives, Offered Storage Array shall support mum 300/600/900/1200 GB hot-pluggable Enterprise SFF SAS hard drives, 400/800/1600GB SSD 2. For LFF drives, offered Storage Array shall support minimum of 4TB / 6TB / 8TB SAS drives. 3. Offered storage array shall be provided with encryption.		
9.	1. Offered Storage Array shall be given with minimum of 6GB cache per controller in a single unit after removing the operating system overhead. 2. Cache shall be backed up in case of power failure for indefinite time either using batteries or capacitors or any other equivalent technology.		

S. No.	Features	Availability (Yes/No)	Remarks
	3. Offered Storage shall also have optional support for Flash cache/equivalent using SSD / Flash drives. Offered storage shall support at-least 400 Gb Flash Cache/equivalent.		
10.	Offered Storage Subsystem shall support Raid 1+0, 5 and Raid 6 with Dual Parity Protection		
11.	Offered Storage array shall be configured with array-based Snapshot and clone functionality and shall be configured for minimum of 64 snapshot licenses. Offered Storage array shall support at-least 512 point in time copies (Snapshots).		
12.	Offered storage subsystem shall support storage-based replication to DR location/ Backup location.		
13.	Offered storage shall be offered and configured with virtualization capability so that a given volume can be striped across all spindles of given drive type. Offered Storage shall be offered and configured with Thin Provisioning capability.		
14.	Offered Storage shall also have optional support for Sub-Lun Data tiering in real time fashion across different type of drives within a given pool like SSD, SAS, NL-SAS etc.		
15.	1. Offered Storage Array shall support Global hot Spare for offered Disk drives.		

S. No.	Features	Availability (Yes/No)	Remarks
	2. At least 2 Global hot spare drive shall be configured for every 30 drives. 3. Storage subsystem shall also have the flexibility to assign dedicated spare for raid sets.		
16.	1. Storage Subsystem shall support minimum of 512 Logical Units. Storage Array shall also support creation of more than 50TB volume at controller level. 2. Offered Storage shall have inbuilt performance management software. Configuration Dashboard shall show overall IOPS and MB/sec performance.		
17.	Multi-path and load balancing software shall be provided, if vendor does not support MPIO functionality of Operating system.		

7.19.6. SAN switch 24 port

S. No.	Features	Availability (Yes/No)	Remarks
Architecture/Scalability/Performance/Management/Availability:			
1.	SAN switches shall be configured where each SAN switch shall be configured with minimum of 12 ports scale up to 24 port.		
2.	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only		

S. No.	Features	Availability (Yes/No)	Remarks
3.	Should deliver 8 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 24 ports in an energy-efficient fashion		
4.	Should protect existing device investments with auto-sensing 4, 8, and 16 Gbit/sec capabilities.		
5.	The switch shall support different port types such as FL_Port, F_Port, E_Port, EX_Port.		
6.	The switch should be rack mountable.		
7.	Should provide enterprise-class availability features such as redundant and hot pluggable components like power supply and FAN		
8.	Non disruptive Microcode/ firmware Upgrades and hot code activation.		
9.	The switch shall provide Aggregate bandwidth of 384 Gbit/sec end to end.		
10.	Switch shall have support for web-based management and should also support CLI.		
11.	The switch should have USB port for firmware download, support save, and configuration upload/download.		
12.	Offered SAN switches shall be highly efficient in power consumption.		
13.	Switch shall support POST and online/offline diagnostics, including RAStrace logging, environmental monitoring, non-disruptive daemon restart, FCping and Pathinfo (FC traceroute), port mirroring (SPAN port).		

S. No.	Features	Availability (Yes/No)	Remarks
Intelligent Networking:			
14.	Offered SAN switch shall support services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expedite high-priority traffic		
15.	The switch shall be able to support ISL trunk up to 128 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.		
16.	SAN switch shall support to restrict data flow from less critical hosts at preset bandwidths.		
17.	It should be possible to isolate the high bandwidth data flows traffic to specific ISLs by using simple zoning		
18.	The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a single fabric.		
19.	Offered SAN switches shall support to measure the top bandwidth-consuming traffic in real time for a specific port or a fabric which should detail the physical or virtual device.		

7.19.7. Racks 42 U

S. No.	Features	Availability (Yes/No)	Remarks
1.	19 inches Rack Mount		
2.	Height of the rack must be 42U or 1.86 meters		
3.	All the racks should be mounted on the floor with castor wheels with brakes (set of 4 per rack)		
4.	All racks must be lockable on all sides with unique key for each rack		
5.	Racks should be compatible with floor-throw as well as top-throw Data Center cooling systems		
6.	Vertically Mounted, 32AMPs with 25 Power Outputs for 5 KVA racks (Racks which have 5 KVA rating)		
7.	A minimum rating of at least 48 AMPS with 25 Power Outputs for 8 KVA Racks (Racks with 8 KVA rating)		
8.	25 Power outs of IEC 320 C13 or C14 Sockets for 5KVA and 8 KVA racks		
9.	Intelligent PDU with remote monitoring using suitable technology such as SNMP		
10.	LED readout for the total current being drawn from the channel. A rack level power consumption readout meter is preferred.		
11.	EIA-310 Standard for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard 19" rack mount equipment.		

S. No.	Features	Availability (Yes/No)	Remarks
12.	OEM racks with Adjustable mounting depth, Multi operator component compatibility, Numbered U positions, Powder coat paint finish and Protective grounding		
13.	Aluminum extruded profile with detachable side panel		
14.	Perforated front and back doors		
15.	All racks should have mounting hardware 2 packs, blanking panel (4U to5U size)		
16.	Heavy Duty Extruded Aluminum Frame for rigidity.		
17.	Duty Top and Bottom frame of MS. Two pairs of 19" mounting angles with 'U' marking.		
18.	Depth support channels - 3 pairs.		
19.	With an overall weight carrying Capacity of mum 500Kgs.		
20.	Fan 230V AC (mum 4 Nos. per Rack)		
21.	Fan Housing Unit mum 4 Fan Position (Top Mounted) (1 no. per Rack-Monitored		
22.	Thermostat based - The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include humidity & temperature sensor		

7.19.8. Access Switch

S. No.	Features	Availability (Yes/No)	Remarks
Access Switch			
1.	24 RJ-45 autosensing 10/100/1000 ports and 2 x 1G/10G SFP+ uplink ports		
2.	Shall have switching capacity of minimum 88Gbps for providing non-blocking performance		
3.	Shall have mum 65million pps switching throughput to achieve wire-speed forwarding		
Architecture			
4.	Shall be 1RU, 19" Rack Mountable		
5.	1 RJ-45 (serial RS-232C) or USB micro-B console port		
6.	Should have 1Gb SDRAM and required flash memory to store min 2 version of operating system & multiple configuration files		
7.	Packet buffer size of mum 12 MB to support video/ streaming traffic		
8.	Shall provide Gigabit (1000 Mb) Latency of < 4 µs		
Resiliency			
9.	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol		

S. No.	Features	Availability (Yes/No)	Remarks
10.	IEEE 802.3ad Link Aggregation Control Protocol (LACP) up to eight links (ports) per group		
Layer 2 Features (any additional licenses required shall be included)			
11.	MAC address table size of mum 16,000 entries		
12.	Shall support IEEE 802.1Q (VLAN IDs)		
13.	Shall support GARP and MVRP VLAN Registration Protocol or equivalent feature to allow automatic learning and dynamic assignment of VLANs		
14.	Shall have the capability to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected, preventing loops		
15.	Shall support 9200 bytes Jumbo frames to improve the performance of large data transfers		
16.	Internet Group Management Protocol (IGMP) as per RFC 1112, RFC 2236, RFC 3376, RFC 4541, RFC 2933		
17.	Multicast Listener Discovery (MLD) snooping as per RFC 2710		
18.	IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and LLDP-MED (Media Endpoint Discovery)		
19.	IPv6 host and Dual stack (IPv4/IPv6) support to provide transition mechanism from IPv4 to IPv6		
20.	Shall support L2 tunneling protocol for network overlay		

S. No.	Features	Availability (Yes/No)	Remarks
QoS and Security Features			
21.	Source-port filtering or equivalent feature to allow only specified ports to communicate with each other		
22.	Shall support traffic classification into eight priority levels mapped to eight queues		
23.	Shall support traffic rate-limiting per port		
24.	Shall support selecting the number of queues and associated memory buffering to meet the requirements of the network applications		
25.	IEEE 802.1x to provide port-based user authentication with multiple 802.1x authentication sessions per port		
26.	Media access control (MAC) authentication to provide simple authentication based on a user's MAC address		
27.	Web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant		
28.	Dynamic Host Configuration Protocol (DHCP) protection to block DHCP packets from unauthorized DHCP servers		
29.	Port security to allow access only to specified MAC addresses		
30.	STP BPDU port protection to prevent forged BPDU attacks		

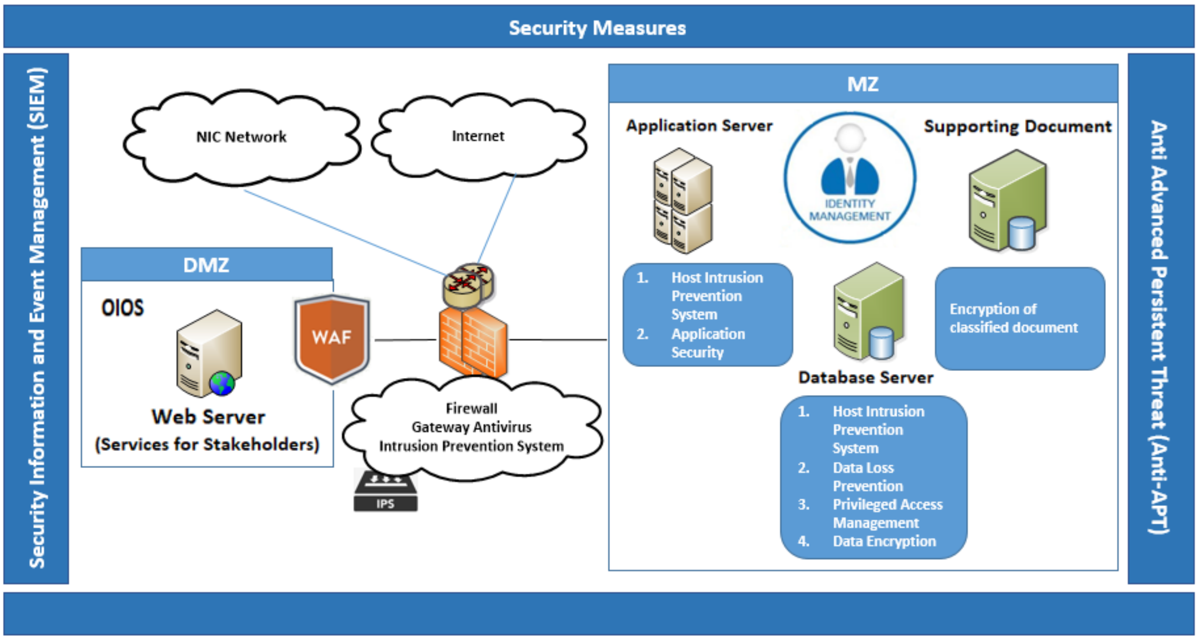
S. No.	Features	Availability (Yes/No)	Remarks
31.	STP Root Guard to protect the root bridge from malicious attacks or configuration mistakes		
32.	Dynamic ARP protection blocking ARP broadcasts from unauthorized hosts		
Management Features			
33.	Configuration through the CLI, console, Telnet, SSH and browser-based management GUI (SSL)		
34.	SNMPv1, v2, and v3 and Remote monitoring (RMON) support sFlow (RFC 3176) or equivalent for traffic analysis		
35.	TFTP, Secure FTP, Zero Touch Provisioning of switch with centralized NMS		
36.	Dual flash images to provide independent primary and secondary operating system files		
37.	Multiple configuration files to allow multiple configuration files to be stored to a flash image		
38.	RADIUS/TACACS+ for switch security access administration		
39.	Simple Network Time Protocol (SNTP) or equivalent support		
40.	Shall have Digital optical monitoring of transceivers to allow detailed monitoring of the transceiver settings and parameters		
41.	OpenFlow 1.3 protocol capability to enable software-defined networking		

S. No.	Features	Availability (Yes/No)	Remarks
42.	Allows the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by an external SDN Controller, utilizing Openflow protocol		
Environmental Features			
43.	Shall support IEEE 802.3az Energy-efficient Ethernet (EEE) to reduce power consumption		
44.	Operating temperature of 0°C to 45°C		
45.	Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC part 15 Class A		
Warranty and Support			
46.	The below Warranty shall be offered directly from the switch OEM.		
47.	5 Year warranty with advance replacement and next-business-day delivery Directly from OEM Only		
48.	Software upgrades/updates shall be included as part of the warranty		

8. Additional Security Requirements

8.1. Security Architecture

SI shall ensure that the product / solution required to implement Security functional requirements (mentioned earlier and in this Section) shall be provisioned/ deployed as part of the overall design. An illustrative minimum-security requirement for OIOS Data Center infrastructure is given below. The SI, however, needs to provide the details of the security architecture with solution to meet the requirement.


Security Measures
Security Information and Event Management (SIEM)
Anti Advanced Persistent Threat (Anti-APT)
NIC Network
Internet
DMZ
OIOS
WAF
Web Server
(Services for Stakeholders)
Firewall
Gateway Antivirus
Intrusion Prevention System
IPS
MZ
Application Server
IDENTITY MANAGEMENT
Supporting Document
1. Host Intrusion Prevention System
2. Application Security
Encryption of classified document
Database Server
1. Host Intrusion Prevention System
2. Data Loss Prevention
3. Privileged Access Management
4. Data Encryption

The OIOS Infrastructure should have multiple security layers to prevent the infrastructure from any external threat. The proposed solution should have different security zones as briefed below and all zones should have physically separate firewall. All firewall policies should be configured based on zone-based requirements.

a. **Militarized security Zone for Production (Database and Application) server Farm (MZ):** This will be a secure Militarize Zone (MZ) to host all critical application, Data Base server, Storage etc. The Zone should not be accessible from Internet directly. All user traffic should be able to enter in this security zone through API's only. The proposed solution should have provision of dedicated Internal Firewall to secure the critical production (Data base and Application) environment.

b. **Demilitarized Security Zone for Web s server Farm (DMZ):** This security zone will host all servers that can be accessed from external world after due authentication and traffic filtering only. This zone shall host the APIs, OIOS Web servers, VPN Concentrator, Access control system, Antivirus Server etc.

2. DMZ should also have honeypot solution to detect security breaches. The honeypot solution should alert the security team when there is a security breach and the team should take the immediate required action to mitigate with the security breach.

c. **Test and development zone (TDZ):** This security zone will host all infrastructure required for test and development. There should not be any access to Production zone from TDZ. This zone should have should be protected by one dedicated firewall pair.

Multilayer security architecture should be proposed to have enhanced network and data security at Data Centers. The minimum Data Center network security requirement is given below:

1. **SIEM (Security Information and Event Management)** – Aggregated picture of all events related to security is provided by a centralized SIEM appliance. SIEM system to enable search, monitoring, analysis, visualization and alerting of log data coming from websites, applications, endpoints, operating systems, servers, network devices, sensors and mobile devices.
2. **Server Patch Management:** Sensitive data resides on servers, remote execution of vulnerabilities in server operating system causes data theft. Patch Management be done to ensure servers are up to date.
3. **Anti-APT (Advanced Persistent Threat)** – Anti-APT proactively gathers information about scouting effort of attacker or group of attackers.
4. **Firewall** – Information is sent to a server from outside world and by server to outside world. Firewall protects the servers from outside users gaining unauthorized access of the environment.
5. **IPS (Intrusion prevention system)** – IPS monitors traffic for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.
6. **Web application Firewall** – WAF is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. While proxies generally protect clients, WAFs protect servers.
7. **HIPS (Host based Intrusion Prevention System)** – Known and unknown attacks occur on servers via software programs targeted to destroy or steal user data on systems based on host name. HIPS monitors host and protects against viruses and malware by monitoring the host for suspicious activities.

8. **Identity and access Management** is a framework to identify, authenticate & authorize a user to access organizational IT resources with complete control on user's accessibility to the resources specific ONLY to the user securing and preventing rest from unauthorized access.

    a. **Two Factor Authentication** – Critical information is stored in the servers and only users granted roles to perform the activity should have access to the specific server by proving their identity by something they know or they are. Two-factor authentication to be used to validate user identity by using combination of different factors matching user provided information.

    b. **SSO (Single Sign-on)** – Users performs day to day activity on servers. To ensure, a valid user is accessing the servers, he should authenticate against his credentials i.e. ID & password to gain access. SSO to be used to authenticate a user against one set of user credentials in the NIC Server (LDAP) or local OIOS environment.

9. **Hardware Security Module:** A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing.

10. **DLP (Data loss prevention)** – Sensitive data is stored on data base/other server. DLP is used to evaluate, monitor and protect occurrences of sensitive information leakage.

11. **SSL VPN (Secure Sockets Layer Virtual Private Network)** – Users connect over the internet to access the department IT services over the internet. SSL VPN to be used for enabling tunnel-based connection to access information via internet securely.

8.2. Security Certification

OIOS Application shall be hosted on DC DR model. **OIOS IT Infrastructure implementation shall be audited by STQC/ STQC empaneled agency before OIOS Phase -II Go-Live**. SI shall be responsible to obtain certification and submission to IAAD.

8.3. Security Solution

8.3.1. Enterprise Network Security

The Enterprise Network Security would include the following security components as single/multiple component(s):

1. Firewall
2. Application Security with user authentication
3. VPN
4. IPS
5. URL filtering
6. Anti-APT Solution with sand-boxing for Internet Zone
7. Threat Prevention

SN	Requirements	Compliance (Y/N)	Remarks
1.	The OEM should fall in the Gartner’s magic quadrant for Enterprise Network Firewalls		
2.	Software defined instance should consist of: • Application based Firewall with SSL VPN • IPS • Gateway Antivirus/ Zero day • Application Security with user identification • URL filtering		

SN	Requirements	Compliance (Y/N)	Remarks
	- Anti APT Note: Solution can be one integrated solution or combination of separate components.		
3.	The security shall be Software/ appliance based.		
4.	The security solution should be application layer (Layer-7) security & user control platform which should be able to identify & prevent known & unknown threats (in real-time basis) covering the related in-scope applications running on the network as per the scope of RFP. The proposed solution should therefore integrate the user's identity repository (across all entities) to enforce authorized access to the related in-scope applications. The solution must be designed to ensure that the performance of the overall applications is not impacted due to the implementation of the security solutions. The Bidder is not required to propose Layer-3 firewalls. The bidder must comply with the technical requirements specified		
Application Security with user identification			
5.	The proposed solution must allow policy rule creation for application control, user-based control, host profile, threat prevention, Anti-virus/ Zero-day, file filtering, content filtering & QoS		
6.	The Solution must support identification and control of all types of applications (Business, Social, Encrypted and Custom) within environment without requiring any license/subscription/blade. It should provide detailed analysis on sessions consumed, data transferred and threats involved through the applications.		

SN	Requirements	Compliance (Y/N)	Remarks
7.	The proposed solution must allow free custom application signatures for Homegrown and custom applications (both current and future) that are running in the network.		
8.	The security instance must support application identification natively, without requiring any license/subscription/blade. There should not be any requirement to buy any license for application visibility and the must operate at Layer 7 natively.		
Security and VPN			
9.	The Security platform should scan files transferred through every application and should not be limited to only HTTP and SMTP and detect applications on all ports.		
10.	The proposed solution must support Policy Based control/forwarding based on: • Zone • Source or Destination Address • Source or destination port • Application (not port based) • AD/LDAP user or User Group • Services or ports		
11.	The proposed solution shall provide Data Loss Prevention - to protect any sensitive information (e.g. Aadhaar number, credit card) leaking out of the network. DLP licenses to be included from day-1.		

SN	Requirements	Compliance (Y/N)	Remarks
12.	The security instance should support both IPSEC and SSL VPN functionality. Licenses to enable the asked number for IPSEC and client-based SSL VPN should be supplied.		
13.	The security instance should support site to site VPN with dynamic and static routing		
14.	The security instance must have a provision to highlight visually the rules which are unused within the policy for a long time.		
Intrusion Prevention System			
15.	Intrusion prevention signatures should be built based on the vulnerability itself. A single signature should stop multiple exploit attempts on a known system or application vulnerability. The proposed security device or its family can also have optional wireless in hardware or software.		
16.	The proposed solution must support different Custom IPS and Application policies for different users and groups. The solution must support FQDN/IP address for static route next hop, policy-based forwarding for next hop and BGP peer address.		
17.	The proposed solution must support different actions in the policy such as deny, drop, reset client, reset server, and reset both client and server.		
18.	Solution should support Session based differentiated services code point (DSCP) classification.		
URL Filtering			

SN	Requirements	Compliance (Y/N)	Remarks
19.	The proposed device shall have custom URL-categorization and support customizable block pages		
20.	The proposed security instance shall have URL Filtering policies by AD/LDAP user, group, machines and IP address/range		
	Should have full-path categorization of URLs only to block re categories the malicious malware path not the full domain or website		
21.	Should have zero-day malicious web site or URL blocking update less than 15 minutes for URL DB update for zero-day malware command and control, spyware and phishing websites access protection		
22.	Should have URL or URL category base protection for user cooperate credential submission protection from phishing attack with malicious URL path		
Anti-APT			
23.	The proposed solution shall have sandbox behavior-based inspection and protection of unknown viruses and zero-day malware for any application and protocol (not limited to HTTP, SMTP, FTP) and the solution shall support automated signature generation for discovered zero-day malware. The solution should support cloud-based analysis. The same should be mentioned on public domain like websites, datasheets.		
24.	Advance unknown malware analysis engine, detecting VM/container-aware malware to detect and protect from virtual sandbox evading advance unknown malware using bare metal analysis.		

SN	Requirements	Compliance (Y/N)	Remarks
25.	Malware Analysis Appliance should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java, PDF etc.		
26.	The proposed security device should be able to detect and prevent zero-day threats infection through HTTP, HTTPS, FTP, SMTP, POP3, IMAP use by any of application used by the users.		
Threat Prevention			
27.	The proposed security instance shall perform content-based signature matching beyond the traditional hash base signatures and should support SMB/ NetBIOS traffic scan/inspection		
28.	All the protection signatures should be created by vendor base on their threat intelligence and should not use any 3rd party IPS or AV engines.		
29.	The proposed solution shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware. Can also have optional wireless support in the software proposed device as well as complete family of OEM.		
30.	The security instance must have a provision to highlight visually the rules which are unused within the policy for a long time.		
31.	OEM must provide performance, throughput and features evidence through public domains- Websites and data sheets only.		

SN	Requirements	Compliance (Y/N)	Remarks
Performance Requirement			
32.	Security instance shall provide application aware throughput of at least 4 Gbps from day one. The OEM must publish performance claims on public domain like websites, datasheets. Letter head performance claims will not be entertained.		
33.	It shall provide threat prevention throughput of at least 2 Gbps from on real world/application Mix/ app mix/ enterprise Mix. The min threat prevention features must include features like IPS, Antivirus, Anti Spyware, Zero Day protection etc.		
34.	Solution must support at least 2 Gbps of IPSEC VPN throughput from Day one without requiring any license.		
35.	The proposed solution must support at least 100 IPsec VPN tunnels and up to 1000 SSL VPN Users from Day one without requiring any license.		
36.	The solution must provide 8 no 10/100/1000 TX interfaces and 1 out of band management interface.		
37.	The solution must provide 8 no 10/100/1000 TX + 4 X 1 Gig SFP and 4x 10Gig SFP+ interfaces populated with desired trans receivers, 2x HA ports and 1 out of band management interface.		

8.3.2. Web Application Firewall

SN	Requirements	Compliance (Y/N)	Remarks
1.	Web Application Firewall should be present in latest Gartner Magic quadrant.		
2.	The proposed WAF can be a dedicated appliance or part of security solution with minimal latency		
3.	Should have throughput to meet functional requirement of OIOS		
4.	Traffic ports as required		
WAF should have the flexibility to be deployed in the following modes:			
5.	Reverse proxy		
6.	The solution must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification.		
7.	WAF should support for IPv4 and IPv6 traffic		
Hiding Sensitive Content Parameters:			
8.	It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social AADHAR)		
9.	It should be able to extract the attack source IP address		
Auto Policy Optimization			
10.	Known Types of Attack Protection		

SN	Requirements	Compliance (Y/N)	Remarks
11.	Zero Day Attack Blocking		
12.	Security Filter Auto Policy Generation		
13.	Working in Learn Mode		
14.	Auto Discovery		
15.	Web Crawler		
Following Threats should be protected by the proposed WAF solution			
16.	a. Parameters Tampering b. Cookie Poisoning c. SQL Injection d. Session Hijacking e. Web Services Manipulation f. Stealth Commands g. Debug Options h. Backdoor i. Manipulation of IT Infrastructure Vulnerabilities j. Buffer Overflow Attacks k. Data Encoding l. Protocol Piggyback m. Cross-Site Scripting (XSS) n. Brute Force Attacks		

SN	Requirements	Compliance (Y/N)	Remarks
	o. OS Command Injection p. Cross Site Request Forgery (CSRF) q. Hot Link r. Information Leakage s. Path (directory) Traversal t. Predefined resource location u. Directory Listing v. Parameter Pollution (HPP)		
The proposed WAF should support the following Security Filters:			
17.	a. Allow List Security Filter b. Brute Force Security Filter c. Database Security Filter d. Files Upload Security Filter e. Global Parameters Security Filter f. HTTP Methods Security Filter g. Logging Security Filter h. Safe Reply Security Filter i. Webservices Security Filter j. XML Security Filter k. Parameters Security Filter l. Path Blocking Security Filter		

SN	Requirements	Compliance (Y/N)	Remarks
	m. Session Security Filter n. Vulnerabilities Security Filter		
The proposed WAF should support the Activity Tracking, which should include the following:			
18.	a. Mimicking user behavior b. Dynamic IP c. Anonymity d. Scraping e. Clickjacking		
WAF should support the Historical Security Reporting			
19.	a. Customizable dashboards, reports, and notifications b. Advanced incident handling c. Standard security reports d. In-depth forensics capabilities		

8.3.3. Security Information and Event Management

SN	Requirements	Compliance (Y/N)	Remarks
1.	The OEM should fall in the Gartner's magic quadrants for Security Information and Event Management		
Administration & Configuration			

SN	Requirements	Compliance (Y/N)	Remarks
2.	The Security Intelligence solution must provide central management of all components and administrative functions from a single web-based user interface.		
3.	The administrator must be able to define role-based access to the system by device, device group or area of network.		
4.	The solution must support auto-discovery of assets/hosts on the network by leveraging both passive network activity data as well as other data sources that feed the Security Intelligence solution (e.g. logs)		
5.	The solution must support automated classification of hosts/assets to enable simplified tuning.		
6.	The solution must support creation and maintenance of a customized list of items that can be referenced by the correlation engine.		
7.	The solution must support the ability to modify communications ports between components.		
8.	The solution must provide an open API for access to data stored within the information database(s).		
9.	The solution must provide the ability to encrypt communications between components.		
10.	The solution must integrate with 3rd party directory systems as an authentication method. How does your solution integrate with a LDAP or AD solution for access provisioning to the SIEM system		

SN	Requirements	Compliance (Y/N)	Remarks
Operational Requirements			
11.	The solution must support the detachment of selected dashboards from the UI for use in SOC or NOC deployments.		
12.	The solution must enable a phased role out of log management and security intelligence functions. Introduction of more analysis capabilities should minimize the need for additional system components and be enabled through license key upgrades.		
13.	The solution must demonstrate 'ease of use'. Ease of use is critical to the successful deployment and on-going use of the solution.		
14.	The solution must support the automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device integration support, etc.		
15.	The solution must support a web-based GUI for management, analysis and reporting.		
16.	The solution must support high availability requirements.		
17.	The solution must ensure all distributed system components continue to operate when any other part of the system fails or loses connectivity. (i.e., management console goes off-line all separate collectors still continue to capture logs).		
18.	The solution must have an automated backup/recovery process.		

SN	Requirements	Compliance (Y/N)	Remarks
19.	The solution should allow storage of logs/configuration files/backup on any storage platform, it shouldn't be proprietary based storage solution.		
20.	The solution must have the ability to employ various storage mechanisms such as local disk, SAN, distributed and load balanced storage, for long-term, short-term, raw, and parsed logs (whichever are applicable). This solution should enable seamless transition between these storage options for ease of use and scalability.		
21.	The solution must automate internal health checks and notify the user when problems arise.		
22.	The solution must provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system.		
23.	The solution must deliver sample dashboards out of the box (i.e. for threat management, compliance management, etc.).		
24.	The solution must maintain a database of all assets discovered on the network. This asset data must include important information about the asset as learned by the information collected (i.e. user identity, system attributes, network attributes, vulnerability state, etc.). The database must provide the ability to edit attributes when they cannot be learned (i.e. department, location, etc.). The user must be able to search this database.		
Architectural Requirements			

SN	Requirements	Compliance (Y/N)	Remarks
25.	The solution must enable deployments as software and/or appliance.		
26.	The solution must integrate with other security and network intelligence solutions.		
27.	The Security Intelligence solution must allow for customization to meet our unique requirements.		
28.	The solution must easily expand to support additional demand. How does your solution scale to increase demand placed on the solution as the organization adds more devices, locations, applications, etc.?		
29.	The solution must support a distributed database for event and network activity collection such that all information can be accessed from a single UI.		
30.	The solution must ensure the integrity of the information collected.		
31.	The solution must provide intuitive mechanisms for troubleshooting such as proactive notifications, command line utilities etc.		
32.	The solution must support a distributed model and give flexibility to write or select predefined correlation rules for correlating counters, sequences, identity lookups, etc.... are shared across all collectors. (i.e., look for 25 login failures from the same user name followed by a single successful login for that same user name, where events seen by a single collector do not exceed the threshold of 25, but across multiple collectors would exceed the threshold).		

SN	Requirements	Compliance (Y/N)	Remarks
33.	The solution must support user extended taxonomy of events and fields. The user must be able to add their own unique event names (i.e., the ability to add in new fields that are not part of the vendors out of the box schema such as a failed called “Special ID from my Custom Application”).		
34.	The solution must allow for custom defined tagging of events.		
35.	The solution must provide transparent retrieval, aggregation, sorting, filtering and analysis of data across all distributed components.		
Log Management Requirements			
36.	The solution must have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage.		
37.	The solution must support log archives on 3rd party storage.		
38.	The solution must provide capabilities for efficient storage and compression of collected data.		
39.	The solution must support industry log collection methods (syslog, WMI, JDBC, LogFile, SFTP, SNMP, Checkpoint LEA, etc.)		
40.	The solution must provide agent-less collection of event logs whenever possible. Does your solution rely on agent technology?		
41.	The solution must provide the ability to distribute both event storage and processing across the entire Log Management/SIEM deployment.		

SN	Requirements	Compliance (Y/N)	Remarks
42.	The solution must support long-term access to detailed security event and network flow data. The system must be able to provide access to at least x months' worth of detailed information.		
Log Taxonomy & Categorization			
43.	The solution must extract common event fields (i.e. usernames, IP addresses, hostnames, and log source device, etc.) from disparate devices across a multi-vendor network and consistently present events in the UI and also give flexibility to add customized fields in cases when SIEM is unable to categorize the events (eq. phone number, Aadhaar card number etc.).		
44.	The solution must support correlation of events from multiple vendor devices, appliances and applications enabling analysis and remediation of high priority threats.		
45.	The solution must provide the ability to store/retain both the log meta data and the original raw message of the event log for forensic purposes.		
46.	The solution must support log time stamps across multiple time zones.		
Event Filtering & Analysis			
47	The solution must provide near-real-time analysis of events.		
48	The solution must provide long term trend analysis of events.		

SN	Requirements	Compliance (Y/N)	Remarks
49	The solution must provide the ability to aggregate an analyze events based on a user specified filter.		
50	The solution must provide more advanced event drill down when required		
51	The solution must provide a real-time streaming view that supports full filtering capabilities.		
52	The solution must provide alerting based on observed anomalies and behavioral changes in network and security events.		
53	The solution must support and maintain a history of user authentication activity on a per asset basis.		
Reporting			
54	The solution must provide reporting on all items available for management via the GUI.		
55	The solution must provide configurable reporting engine for customized report creation.		
56	The solution must support the ability to schedule reports.		
57	The solution must provide templates for the easy creation and delivery of reports at multiple levels ranging from operations to business issues.		
58	The solution must provide 'canned' out-of-the-box reports for typical business and operational issues.		

SN	Requirements	Compliance (Y/N)	Remarks
59	The solution must provide ‘canned’ out-of-the-box reports for specific compliance regulations (PCI, SOX, FISMA) and control frameworks including (NIST/ CoBIT/ ISO).		
60	The solution must provide a ‘Dashboard’ for quick visualization of security and network information.		
61	The solution must support the automated distribution of reports.		
62	The solution must support the capability to provide historical trend reports.		
63	The solution must support the ability to centrally deliver vulnerability reports.		
64	The solution must support the ability to centrally deliver asset reports.		
Correlation and Alerting			
65	The solution must provide alerting based on observed security threats from monitored devices.		
66	The solution must provide the ability to correlate information across potentially disparate devices.		
67	The solution must provide alerting based on observed anomalies and behavioral changes in network activity (flow) data.		
68	The solution must provide alerting based upon established policy. (e.g., IM traffic is not allowed.)		

SN	Requirements	Compliance (Y/N)	Remarks
69	The solution must support weighted alerts to allow for prioritization. Weights must be assignable based on multiple characteristics such as asset type, protocol, application, etc.		
70	The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions		
71	The solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.		
72	The solution must limit the presentation of multiple similar alerts.		
73	The solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.		
74	The solution must integrate with security and threat intelligence feeds data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.) for the purpose of correlating internal activity with external threats. These data feeds should be updated automatically by the solution		
75	The solution must support the ability to correlate against 3rd party vulnerability scan results.		
76	The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in X minutes then generate an alert.		

SN	Requirements	Compliance (Y/N)	Remarks
77	The solution must support correlation for a missing sequence. Example service stopped not followed by the service restarting within 10 minutes.		
78	The solution must support correlation for additive values over time. For example, alert when any SRC IP sends more than 1GB of data to a single port on a single DST IP in a one-hour period of time.		
79	The solution must be able to pull in identity context from variety of sources in order to appropriately map user identity with current activity. Solution must be able to map multiple user aliases/attributes back to a single user.		
80	The solution must provide a mechanism, to optimize rule tuning, which allows for the grouping of similar input values of a correlation rule that can be used by multiple rules. This grouping mechanism should allow for both static groups and groups that are dynamically created by other correlation rules. For example, the user of the system can define a group of banned ports/protocols that should be used across multiple correlation rules that monitor for inappropriate network activity.		
SIEM Workflow			
81	The solution must provide the ability to send notification of correlated alerts via well-defined methods (i.e. SNMP trap, email, etc.)		
82	The solution must provide embedded workflow capability that security operations staff can use to guide their work		

SN	Requirements	Compliance (Y/N)	Remarks
83	The solution must provide integration with 3rd party trouble ticketing/help desk systems that security operations staff may use to guide their work		
84	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, vulnerability data, etc.		
85	The solution must provide a mechanism to annotate a security incident as it is addressed by the security operations staff.		
86	The solution must provide a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.). The user must be able to filter incidents along these defined attributes.		
87	DNS Malware Monitoring: The vendor's solution must provide ability to detects malware-infected hosts and endpoints—servers, desktops, mobile devices—rapidly with high fidelity. Solution must provide following details: • Top domain shared by infected clients • Most queried blacklisted domains • Top Malware Types • Top IPs and Subnets		

SN	Requirements	Compliance (Y/N)	Remarks
88	DNS Malware Analytics Techniques: The vendor's solution can detect malware infected systems through DNS calls out to malicious domains. It should be positioned as a detection solution. DNS Malware Analytics can determine malicious domains through the following techniques: 1. Blacklists – these can point to a number of malware types that are typically passed from a particular Black List Domain. 2. Domain Generating Algorithm – this algorithm detects whether malware might have generated the Domain through a random text generator. 3. Frequency Analysis – this analytic detects malware behavior by the number of malware C&C events over a time domain. 4. Length of Domain Analysis – this analytic detects the randomness and length of Domain (data exfiltration) 5. A combination of these Analytics		
89	Attack Visualization: The vendor's product must provide the ability to visually represent event data into a dynamically updated graph. This will assist analysts in determining the expanse of attacks and pinpoint the original attacker during incident response and remediation. For example, • Event Graph • Geo Event Graph • Last State		

SN	Requirements	Compliance (Y/N)	Remarks
90	Collection Load Balancing: The vendor's product must provide options for load balance incoming logs to multiple lo collector instances. It should at least load balance syslog events.		
	Application Security Logging and Monitoring: The vendor's product must provide option to monitor security vulnerability through application security logging even logs are not natively generated by applications.		

8.3.4. Data Loss Prevention (System administrators console)

SN	Requirements	Compliance (Y/N)	Remarks
1.	The solution should be in Gartner Leaders Quadrant of Enterprise Data Loss prevention.		
Data Loss Prevention (DLP) for Endpoints			
2.	DLP Solution should actively monitor the ways confidential data can be used on the endpoint and flags any activity not in accordance with policy defined from the centralized console.		
3.	DLP Solution should provide choices to address and remediate incidents and use technology specifically designed to operate in the most efficient and unobtrusive manner possible.		
4.	DLP Solution should scan laptop and desktop hard drives for confidential/Sensitive data in order to inventory, secure or relocate it		

SN	Requirements	Compliance (Y/N)	Remarks
	and provide templates or equivalent to enable out-of-the-box discovery of sensitive data mapped to different industry and regulatory directives.		
5.	DLP Solution should scan for confidential/sensitive data when endpoint is idle and subsequent scans must run on only those things that have changed since the previous scan.		
6.	DLP Solution should provide following detection technologies to address different types of data: Content which looks for data matching keywords, expressions or patterns, file type recognition, and other signature-based detection technologies. Fingerprinting which looks for exact matches of whole or partial files, coming from structured sources (e.g., databases) and unstructured sources (e.g., design documents) that are fingerprinted with a hashing algorithm. Learning technology to identify unstructured data such as source code, Intellectual Property (IP), or legal contracts by building a statistical model based on uploading positive and negative example documents.		
7.	Fingerprinting which looks for exact matches of whole or partial files, coming from structured sources (e.g., databases) and unstructured sources (e.g., design documents) that are fingerprinted with a hashing algorithm.		
8.	Learning technology to identify unstructured data such as source code, Intellectual Property (IP), or legal contracts by building a statistical model based on uploading positive and negative example documents.		

SN	Requirements	Compliance (Y/N)	Remarks
9.	DLP Solution should prevent confidential/sensitive files from downloading, copying to CD/DVD/USB/iPod®/Bluetooth®, and other removable media; print screens, communications over email.		
10.	DLP Solution should monitor and prevent data using HTTP/HTTPS over browsers like Chrome, FireFox and Explorer at endpoint.		
11.	DLP Solution should monitor data being copied and pasted from the clipboard to prevent confidential/sensitive data from being pasted to specific application.		
12.	DLP Solution should provide trusted device support enables organizations to define specific removable media devices that can be used with confidential data, providing a more granular level of protection while still enabling required business functions.		
13.	DLP Solution should provide application file access control to secure the use of confidential/sensitive data applications like social web sites when on internet.		
14.	DLP Solution should provide broad remediation capabilities: onscreen pop-up notifications; quarantining or relocating data to a secure location; blocking endpoint events; and applying custom responses via the flexible response feature, such as applying encryption to a file using the endpoint encryption flex response.		
15.	DLP Solution should automatically notify data owners of this policy violation.		

SN	Requirements	Compliance (Y/N)	Remarks
16.	Solution should detect whether data has been entered in forms such as tax, medical, or financial forms in various image formats like PDF, JEPG, BMP, PNG and TIFF.		
17.	Should be able to exclude specific printers from being monitored, including local, network, and PDF printers.		
18.	DLP Solution should have a web base management for defining, deploying, and enforcing data loss policies, responding to incidents, analyzing and reporting policy violations, and performing system administration.		
Data Loss Prevention (DLP) for Mail at SMTP			
19.	DLP Solution should monitor mail communications and detects confidential/sensitive data that is being sent in violation of security policy. If a security policy is violated, it should block email communications.		
20.	DLP Solution must redirect, quarantine, or block outbound messages containing confidential/sensitive data. It must be deployed at egress points in the network DMZ and should integrate with your existing on-premise messaging infrastructure.		
21.	DLP Solution should quarantine or relocate email containing sensitive data to a secure location for end-user review and release.		
22.	DLP Solution should provide broad integration support for enterprise messaging gateways, Mail Transfer Agents (MTAs).		

SN	Requirements	Compliance (Y/N)	Remarks
23.	DLP Solution should scales to hundreds of thousands of global network users DLP for Mail should have integration with antispam solution using standard SMTP.		

8.3.5. Host Intrusion Prevention System

SN	Requirements	Compliance (Y/N)	Remarks
1.	The OEM should fall in the leaders' Quadrant of Gartner's magic quadrant for Endpoint Protection Platforms.		
2.	Protection from all classes of attacks, including port scans, buffer overflows, Trojan horses, and worms.		
3.	Automated real-time intrusion detection and should protect by analyzing the events, operating system logs and inbound/outbound network traffic on enterprise servers		
4.	There should be a separate Management Center for Server Security Agents which will provide all management functions for all agents in a centralized manner and should allow creation of custom and location-based policies.		
5.	The HIPS should offer an enterprise-scalable architecture; the HIPS should be scalable to thousands of agents per manager		
6.	The HIPS should use the HTTP and SSL protocols for the management interface and for the communication between the HIPS and		

SN	Requirements	Compliance (Y/N)	Remarks
	management center. The HIPS should reside between the applications and the kernel, enabling maximum application visibility with minimal impact to the stability and performance of the underlying operating system		
7.	When an application attempts an operation, the HIPS should check the operation against the application's security policy, making a real-time allow or deny decision on its continuation and determining if logging the request is appropriate.		
8.	By combining security policies implementing firewall, operating system lockdown and protection, and audit event collection capabilities in default policies for servers, the HIPS should provide defense-in-depth protection for exposed systems.		
9.	Correlation should be performed both on the agent and on the Management Centre console. Agent based correlation should be supported. The Management Centre for HIPS should provide all management functions for all HIPS agents in a centralized manner from the security management software to be provided by the bidder.		
10.	Should protect the end points even when they are off network.		
11.	Should be compatible with the chosen operating system and server hardware.		
12.	HIPS should provide a user-friendly interface.		
13.	HIPS will be deployed at all the servers at the Primary site and the DR site.		

SN	Requirements	Compliance (Y/N)	Remarks
14.	HIPS should prevent external USB/CD/DVD drivers		

8.3.6. Privilege Mgmt. of System Administrator (VMs, Physical Servers, Storage)

SN	Requirements	Compliance (Y/N)	Remarks
Privileged Account Management System-Agentless			
1.	The proposed could be either: appliance-based, virtual appliance based.		
2.	User's access to the proposed solution should be via encrypted channel only.		
3.	Upon logged in, the propose solution should only display credentials that the user have access to, based on a zero trust, explicitly allow only model.		
4.	The proposed solution should allow Agency to secure, manage, automate and log all activities associated with the privileged accounts for audit trail purpose.		
5.	The proposed solution should support scheduled password changes based on Agency's requirement.		
6.	The proposed solution should be appliance-based solution with no overhead of installing each component separately.		

SN	Requirements	Compliance (Y/N)	Remarks
7.	The proposed solution should share a common infrastructure for managing, securing and tracking shared privileged accounts.		
8.	The proposed solution should be browser independent and there shouldn't be any browser dependency to manage and record the sessions.		
9.	The proposed solution should allow whether to enforce users to specify reason when requesting access for a privileged account.		
10.	The proposed solution should allow specifying automatic password changing for a privileged account each time after it is used.		
11.	The proposed solution should be policy based and can be configured different policies for different platform privileged accounts.		
12.	The PIM solution should have wizard-based integration with third party solutions like RADIUS/LDAP/SYSLOG etc.		
13.	The proposed solution should have alert system for: Alert the Approver when a new request has been put up for his approval.		
14.	The proposed solution should have the ability to contain users to have access and visibility to authorized resources only.		
15.	The proposed solution should support integration with enterprise infrastructure including strong authentication such as 2-factor, Radius, RSA, LDAP and RSA + LDAP, PKI, Composite auth (LDAP+RADIUS or LDAP+RSA)		

SN	Requirements	Compliance (Y/N)	Remarks
16.	The proposed solution should support communications with LDAP-compliant directory servers to obtain user identification and security information. This validation process should be done at the second factor authentication server to reduce redundancy and ease of deployment.		
17.	The proposed solution should provide web browser-based interface for users to perform activities related to privileged account such as request, approval and audit trail retrieval.		
18.	The proposed solution should support dual approvers control as part of the workflow for privileged account password request, if required.		
19.	The proposed solution should provide secure remote access to sensitive servers such as Windows servers, Unix/Linux, iSeries and network devices without having to expose credentials to end-users e.g. external vendors.		
20.	The proposed solution should log all administrative tasks that were done on the proposed system for audit trails purpose.		
21.	The proposed solution should enable extraction and archival of audit logs.		
22.	The proposed solution should generate complete audit trail reports for management review.		
23.	The proposed solution should generate compliance audit trail reports for reviewing.		

SN	Requirements	Compliance (Y/N)	Remarks
24.	The proposed solution should have session timeout capabilities, when session ideal and this parameter should be in configurable mode.		
25.	The proposed solution should support logs forwarding to support the SIEM operations		
26.	The Proposed solution should have ability to manage Windows, Unix, CISCO IOS, Juniper JUNOS, AS400, MSSQL, Oracle, ESX/ESXi local administrator credential through single appliance.		
27.	The Proposed solution should have ability to define a zero trust, explicitly allow only access methodology.		
28.	The Proposed solution should have ability to support up to 2000 concurrent RDP session with Session recording feature enabled.		
29.	The Proposed solution should support Active-Active High Availability (HA) architecture without the use of a traffic load balancer.		
30.	The Proposed solution should have ability to provide real-time data synchronization among a cluster.		
31.	The Proposed solution should have ability to block and deny bash shell commands without the usage of any agent-based solution.		
32.	The proposed solution should offer in various forms: appliance-based, virtual appliance based.		
33.	Secure Remote Access Facility - The Secure Remote Access facility is to provide an encrypted channel for users to connect to the target servers		

SN	Requirements	Compliance (Y/N)	Remarks
	using the privileged accounts retrieved from the above Privileged Account Management system. It shall also record all activities done by the users on the target servers.		
34.	The proposed solution should create isolation between the privileged user's desktop and the target system, which eliminates the risk of planting malware on critical systems.		
35.	The proposed solution should tightly integrate with the Privileged Account Management system such that it can be launched from the Privileged Account Management system and without having to expose credentials to end-users e.g. external vendors.		
36.	The proposed solution should provide secured access to the target servers through mechanism such as encryption.		
37.	The proposed solution should control, monitor and record privileged sessions including RDP, SSH, Telnet, HTTP/HTTPS, AS400 and Mainframe in single module.		
38.	The proposed solution should be able to support application-based session via RDP protocol.		
39.	The proposed solution should be able to map local drive or directory during an RDP session.		
40.	The proposed solution should be able to auto discover devices in the network segment range.		

SN	Requirements	Compliance (Y/N)	Remarks
41.	The proposed solution should be able to integrate with VMware Vcenter to auto- discover and provision VM images onto the device list.		
42.	The proposed solution should provide full session recording.		
43.	The solution should have the ability to perform SHA verification every time the session recording is being played to ensure the session recording integrity is not compromised.		
44.	The proposed solution supports more than 2000 concurrent session recordings (*) by a single server. Note: *SI need to synchronize it with as per proposed solution		
45.	The proposed solution should provide facility with proper access control mechanism for the retrieval and viewing of the recorded privileged sessions.		
46.	The proposed solution should compress the session recordings to reduce the need for excessive storage.		
47.	The proposed solution should support privacy regulation by allowing on-screen user notification when a session is being recorded.		
48.	The proposed solution should be able to support text searching for SSH sessions.		
49.	The proposed solution should be able to prevent leap frog attempts.		
50.	The proposed solution should be able to blacklist or whitelist commands during command line-based session.		

SN	Requirements	Compliance (Y/N)	Remarks
51.	The proposed solution should support the use of native SSH client, e.g. Putty, by creating a SSH tunnel through the proposed solution and still able to blacklist or whitelist command, SSO, and record session.		
Backup / Upgrade / Redundancy / High Availability			
52.	The proposed solution should have the ability to support auto load balancing and active- active high availability (HA) out-of-the-box to cater for current requirements and future expansion.		
53.	The proposed solution should allow for backup of the policies that is set in the proposed system which can also be easily imported to another proposed system.		
54.	The proposed solution should be highly scalable and performance oriented.		
55.	The proposed solution should have easy wizard-based upgrade process to ensure near zero downtime while upgrading the PIM solution.		
Accreditation			
56.	The proposed solution must be at least accredited with:		
57.	FIPS 140-2 Level 2 validated cryptography, able to achieve FIPS 140-2 Level 3 with built- in hardware security module (HSM)		
58.	Common Criteria EAL 4+		
Documentation and Knowledge Transfer			

SN	Requirements	Compliance (Y/N)	Remarks
59.	The supplier shall provide documentation on all provided systems with detailed instructions on the installation, setup and customization.		
60.	The supplier shall provide training for the System Administrators as well as users for the proposed systems.		
A2A			
61.	The proposed solution should provide the capability to manage application credential together with access control and password management all within a single hardened platform.		
62.	The proposed solution should provide a client that is either 32bit or 64bit		
63.	The proposed solution client should support the following platform AIX 5.2, 5.3, 6.1, SUSE 9, 10, 11, Solaris 8, 9, 10, Windows Server 2003, 2008, Red Hat AS 7.2, Red Hat Enterprise 4.0, 5.1, OS/400, HPUX 11i and/or z/Linux etc.		
64.	The proposed solution should support locally cache credential to reduce network traffic and increase reliability		
65.	The proposed solution should support silent installation of the application credential management client onto the Linux, Unix or Windows server		

8.3.7. Database activity monitoring

SN	Requirements	Compliance (Y/N)	Remarks
1.	Solution should perform monitoring of queries, objects and stored procedures with real-time alerts		
2.	The administration of the solution should support segregation of duties based on roles/groups etc. The roles can be defined so that no one can have extensive privileges on the solution		
3.	Should have built in Vulnerability Assessment module to capture database vulnerabilities and monitor the same		
4.	The solution should be able to integrate with LDAP		
5.	The solution should support virtual environments		
6.	The solution should be able to auto-discover all databases objects in the desired network.		
7.	Should alert if any credit card numbers and any other field defined by CAG as important fields are recorded in database transactions		
8.	Solution should be able to auto discover default passwords in the default DB accounts.		
9.	Should be able to block users based on policies		
10.	The solution should inspect both in-coming and out-going DB traffic and compare with the rules		

SN	Requirements	Compliance (Y/N)	Remarks
11.	Should have the ability to mask or obfuscate Sensitive Production Data in the result sets to the user.		
12.	Ability to kill sessions for accessing sensitive data/policy violations and keeping all activity in the logs.		
13.	The solution should be able to block attacks like SQL Injection, Denial of Service in real time and generate alerts.		
14.	The solution should be capable of monitoring all activities pertaining to all in scope databases for all types of users, through network or at the host including login/log off. All DDL/DCL/DML commands/SQL transactions, all administrator commands such as Grant, Revoke etc., details of stored procedures executed should be captured (executed by, procedure name, time of execution, tables accessed etc.)		
15.	The solution should be able to integrate with SIEM		
16.	The solution should have reporting/integration capabilities through syslog/SNMP		
17.	Solution should provide centralized audit repository for audit data collected from multiple database types. The log files should be stored within the solution. It should be tampering proof.		
18.	Should be able to collect, aggregate and normalize activity logs from various databases.		
19.	Should include reports highlighting segregation of duty issues for DBAs		

SN	Requirements	Compliance (Y/N)	Remarks
20.	Should be able to share reports through email, syslog, etc.		
21.	Should be able to control access to database on the basis of source IP(s)		
22.	Should be able to recognize a higher volume than normal transactional volume from a particular user and generate alerts		
23.	Should provide for policy creation to address specific queries, result counts, administrative functions (new user creation, rights changes), signature-based SQL injection detection, UPDATE or other transactions		
24.	Should also provide for heuristics-based policy creation and vendor should assist Bank with tuning of these policies		
25.	The solution should be able to auto-discover all databases objects in the desired network.		
26.	The solution should be able to auto discover privilege users in the database.		
27.	The solution should be able to auto discover default passwords in the default DB accounts.		
28.	The solution should discover if any new database and DB objects created within the monitored network/systems.		
29.	The solution should be capable of auto-discovering sensitive/confidential data, like credit card nos., in the database objects and reporting operations on this data as per defined rules.		

SN	Requirements	Compliance (Y/N)	Remarks
30.	The solution should provide easy pre-defined policy/rule creation templates.		
31.	The solution can be configured to support both detection and prevention of activities.		
32.	The solution should have capability to facilitate rule creation at a very granular level. Example: Which user can connect from which source, access what objects, have which rights, at what time window etc.		
33.	Rules also should allow blocking access depending upon different parameters like above.		
34.	Automated mechanism for updating security configurations/policies across multiple databases.		
35.	Can track and alert on all failed logins.		
36.	Can track the dormant accounts as per defined rule.		
37.	The solution should be able to schedule and distribute the reports on demand.		
38.	Solution should be capable of tracking, identifying and logging activities performed by DBA (without network access, using OS authentication) through the console.		
39.	The solution should capture and store the contents of all commands and the output of the commands.		

SN	Requirements	Compliance (Y/N)	Remarks
40.	The solution should support creation of user defined reports without using any third-party solution.		
41.	The solution should be capable to have an executive dash board to provide a summary view basing on user defined criteria.		
42.	Reporting can be done at a very granular level, like all the activities for a user, all the activities for a system with filtering capabilities. (on IP, time, command etc.)		
43.	The solution should be able to generate the reports in HTML, PDF, Excel formats as per requirement of the user.		
44.	The solution should provide full details needed for analysis of audited events: date and time, raw SQL, parameters used, end user name, source IP, source application, destination database instance, schema DB objects affected, command details, results generated, values affected etc. Should be capable of capturing and reporting at a very granular level.		
45.	The solution should discover miss-configurations in the database and its platform and suggest remedial measures.		
46.	The solution should capable of doing a vulnerability assessment test on the database and report the same with remedial measures		
47.	The solution should be capable of reporting missing patches and report the details of such patches and vulnerabilities associated with.		

8.3.8. Hardware Security Module

Use case for HSM is to store keys for encrypting Aadhar data. HSM solution needs to be offered on PaaS subscription model.

SN	Requirements	Compliance (Y/N)	Remarks
1.	HSM shall be PaaS, pay-as-you-go business model		
2.	OS Support: • Offered OS for OIOS • Windows Server latest version • RHEL Latest version		
3.	The solution should be able to protect data-at-rest, data-in-motion, classified data against root privileged user account access. It should also protect file, folder level encryption.		
4.	Solution should support fine-grained policy to enable administrator to perform activity like file archive and backup, without access to the data content itself.		
5.	Proposed solution should support multi-tenancy using separate domain with configurable policies, data encryption key management and audit log.		
6.	Should have comprehensive logging and reporting functionality		
7.	Should have a seamless SIEM Integration		
8.	Container Support – OIOS Solution (if container is used), Docker, Red Hat Open Shift		

SN	Requirements	Compliance (Y/N)	Remarks
9.	Network Management support- SNMP, NTP, Syslog-TCP		
10.	The data transformation should not involve any downtime and live transformation is expected to achieve high Performance Encryption with 100% System Uptime.		
11.	Non-disruptive key rotation.		
12.	Key rotation can be done on live transformation of data with no downtime.		
13.	Administrator of Key Manager should strongly authenticate using RSA 2FA solution		
14.	Should integrate with users and groups from LDAP, local systems, container environments etc.		
15.	The package must include a single management (Device Manager) application to install and configure HSM devices.		
16.	The HSM must comply with current GoI, CCA guidelines		
17.	FIPS 140-2 Level 3 compliant		
18.	Sizing: Storage of key values should be as per OIOS solution requirement		

8.3.9. Anti-Virus malware and Anti-Spam (for Server & System administration OS)

SN	Requirements	Compliance (Y/N)	Remarks
1.	Solution should be in Leaders magic quadrant of Gartner		
2.	Solution should analyze incoming data and blocks threats while they travel through the network before hitting the system. Rules-based firewall and browser protection should be included to protect against web-based attacks.		
3.	Solution should have signature-based antivirus should eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits.		
4.	Solution should correlate linkages between users, files, and websites to detect rapidly mutating threats. By analyzing key file attributes, Solution should accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks.		
5.	Solution leverage artificial intelligence to provide zero-day protection and stop new and unknown threats by monitoring malicious file behaviors while they execute in real-time to determine file risk.		
6.	Solution should provide protection for business-critical systems by only allowing whitelisted applications (known to be good) to run or by blocking blacklisted applications (known to be bad) from running. Finger printing of applications should be from centralized console.		
7.	Solution should help identify and protect internal and external security breaches by monitoring application behavior and controlling file access, registry access, processes that are allowed to run, and devices information can be written to.		

SN	Requirements	Compliance (Y/N)	Remarks
8.	Should allow administrator to verify and report compliance; quarantine location and peer-to-peer enforcement lockdown and isolate a non-compliant or infected system.		
9.	Should automatically detects what location a system is connecting from, such as intranet and internet and adjusts the security to offer the best protection for the environment.		
10.	Solution must prevent clients from downloading full definition packages.		
11.	The solution should download content updates when computers are idle. Following conditions should be monitored to check whether the client is idle: The user is not idle The computer is on battery power. The CPU is busy. The disk I/O is busy. No network connection is present.		
12.	Solution should automatically switch to aggressive scan mode if windows client detects a large number of viruses, spyware, or high-risk threats to clean/delete/quarantine these threats.		
13.	Solution should provide graphical display to manage and monitor content distribution providers or group update providers in our environment. It should also provide health and content distribution status of group update providers.		

SN	Requirements	Compliance (Y/N)	Remarks
14.	Solution should able to collect file fingerprints for all the applications that a group of client computers run for whitelisting or blacklisting.		
15.	Solution should provide rich set of reports for management and administrators.		
16.	Solution should be support windows and Linux Operating Systems.		

8.3.10. Identity Access Management

SN	Requirements	Compliance (Y/N)	Remarks
1.	Software as a Solution (SaaS) offering		
2.	Should integrate with existing LDAP data		
3.	Supports Identity Creation with associated identifiers and credentials		
4.	Should support automated account creation, suspension, and deletion across systems and applications based on changes in the relationships a given individual has with the organization with these Identity Management activities to be governed by Roles and Entitlements		
5.	Supports Identity Modification and Update to reflect changes in identity attributes and associated identifiers and credentials		
6.	Should support synchronization of identity information to various repositories/ directories based on an "authoritative source" model		

SN	Requirements	Compliance (Y/N)	Remarks
7.	Should support Synchronization of IDs and passwords across platforms and applications		
8.	Supports Identity merging and splitting		
9.	Supports delegated Identity administration		
10.	Supports configurable password policies		
11.	Supports self-service password resets		
12.	Supports account reconciliation		
13.	Supports data synchronization with other data stores		
14.	Supports platform specific provisioning and de-provisioning connectors		
15.	Supports access request management. Ability to provide a consistent and auditable process for requesting access		
16.	Should have robust reporting capability to include ad hoc reporting.		
17.	Single-Sign on technology to manage all credentials of a given user across many technology platforms including web and non-web-based applications		
18.	The application supports session context step-up from password authentication to 2-factor token authentication when more sensitive data or functions are requested by a user.		

8.3.11. Single Sign-on (SSO)

SN	Requirements	Compliance (Y/N)	Remarks
1.	The Product must support Open Standards like SAML 2, oAuth 2, OpenID Connect, WS-Security and WS Federation		
2.	Should integrate with existing LDAP (managed by NIC)		
3.	The Product must support Implementation of SAML 2 Identity Provider and SAML 2 Service Provider for authentications based on SAML2		
4.	The Product must support Implementation of oAuth2 Authorization Server and Resource Server for authentications based on oAuth2		
5.	The product should support secured communication between different components using SSL		
6.	The Solution should support global idle session timeout, session timeout for idle sessions and single log-out		
7.	Support for SSO to legacy applications		
8.	Should integrate with SIEM and other security, application components.		
9.	Support for SSO using reverse proxy		

8.3.12. Access Control and Authentication Specifications

SN	Requirements	Compliance (Y/N)	Remarks
1.	Solution must provide access to only those applications/resources that the user is authorized to.		
2.	Once a user has been authenticated to the sign on system, access to all authorized Web applications and resources must be handled by this system.		
3.	Solution must provide capabilities to ensure dual factor authentication for re-authentication or sensitive resource access.		
4.	Priority of these authentication methods should be Administrator specified. It should not be hard-wired into the product and Administrator should be able to control the priority of each authentication method.		
5.	The application should support time or location-based policies.		
6.	Administrator should be able to create a policy for any user, any group (including dynamic groups), any role, or even any ad-hoc set of users who share certain attributes.		
7.	Solution should support automatic failover and failover between clusters.		
8.	The proposed solution must provide API that should support workflow capabilities.		
9.	Solution must ensure all user credentials are encrypted in storage (local) and in transit between all components of the system		

SN	Requirements	Compliance (Y/N)	Remarks
10.	Should be provided for not only the users accessing the applications from PCs but also from other devices such as PDAs, Mobile phones etc.		
11.	Solution should include LDAP v3 compliant directory system support Directory Synchronization in order to synchronize the user credentials with central repository. The type of synchronization can be event based or timer based.		
12.	The solution should adhere to standards for ease-of-integration with existing systems and future IT investments. Native support for known industry standards, such as JAAS, J2EE, LDAP, PKIX, SSL, etc		
13.	Solution should support both thick client and web-enabled applications.		
14.	Solution should support risk and knowledge base authentication and will be able to create challenge response in case of any change in user behavior.		

Note:

1. It is to be noted that bidder has to provide availability/compliance of every component as indicated in this document. The mentioned specifications may not be taken as an exhaustive list and is only giving a framework for preparing the solutions. Bidder can propose higher specification while designing the solution. Any additional component / functionality to meet the solution requirements should be assessed and included by the bidder as part of the overall solution.
2. Availability/compliance (yes) of all the components should be provided with cross-referencing linked to publicly available documents. Bidder needs to refer to relevant pages and paras of datasheet in the remarks' column. In case, the availability/compliance of a particular

component is in ‘negative’, the bidder needs to explain why/how the non-availability/non-compliance of that component would not impact the design/performance of the OIOS Solution.

3. Bidder needs to submit the cross-referenced related OEM document to confirm the compliance to the requirement.

--------------End-----------------

Comptroller and Auditor General of India

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Request for Proposal

`Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

'One IA&AD One System' (OIOS) Project

VOLUME – I – Annexure D

Reference Number: 51-ISW/2019-'One IA&AD One System' Project

1. Table of Contents

2. Annexure D – Indicative key data points

The indicative key data points relating to the OIOS IT solution are detailed in this document. The data points mentioned below are indicative in nature from the system design perspective. The bidder needs to validate this data and do their own estimation. IA&AD does not take any responsibility for the accuracy of the data points and sizing as these may undergo change.

2.1. Number of field audit offices

Currently, the total number of field audit offices including branch offices is about 156. The stream-wise split of the number of field audit offices has been listed in the Table below. As explained in RFP Vol I document, a total of 31 field audit offices have been selected as ‘pilot’ and ‘nodal’ offices. However, it is important to note that the number of field audit offices would undergo a change with any administrative re-structuring that is taken up by IA&AD. The system design of OIOS should allow for the required scalability and should be agnostic towards the administrative structure of IA&AD. The OIOS IT solution should treat the office structure in such a way that the restructuring of IA&AD does not result in “Change management”, but will be managed through re-configuration.

Table 1: Field audit offices in IA&AD

Field audit offices of IA&AD		
Audit of the Union Government		**52**
Civil audit	12	
Defence audit	6	
P&T audit	1	
Railways audit	18	
Commercial audit	12	
Overseas audit	3	
External audit		**1**
Audit of the State Governments		**41**
Total (excluding branch offices)		**94**
Approximate number of branch offices		**62**
Total (including branch offices)		**156**

2.2. Number of users in IA&AD

The total number of users is expected to be around 30000 (see Table below). Among the 30,000 users, approximately 23,750 users would be core-users with the others being only occasional users, if at all. The total number of concurrent users is estimated at 10%, taking the number of concurrent users to 2375 users. Presently, there is a 23% vacancy in the total sanctioned strength of employees. Hence, the OIOS IT solution should provide for scalability of an additional 23% of users. This works out to be 39,000 users - 29,200 core users and 2,920 concurrent users.

Table 2: Manpower position

	Total	HQ	Field
Total Users	**29,693**	**15,223**	**14,470**
Core users (excluding S. No. 5)	23,731	9,261	14,470
Concurrency (10%)	2,373	926	1,447

2.3. Data sizing

The data sizing may be divided into three categories, viz. a) Application data (including meta-data and workflow data) b) key documents c) Audit products and d) Auditee information. Since, this is the first enterprise level application that is envisaged to be rolled out, IA&AD is not in a position to size application data requirements. IA&AD is also not in a position to size the volume of Auditee Information, since we do not have historic information on this. However, the indicative sizing for key documents and audit products are detailed below.

2.3.1. Key documents

The sizing of the key documents based on assignment types is detailed below. It is important to note that the sizing per assignment is only approximate. The data retention time period is around 25 years. However, the OIOS IT solution should provide a scalability of at least 07 times (expected lifespan of the hardware).

Sizing of Key documents (per year)

Nature of assignment	Number of assignments[1]	Sizing per assignment	Total sizing (Approximate)
Units covered under compliance audit assignments	56,692	50 MB	3 TB
Performance audit assignments	116	10 GB	1 TB
Financial audit assignments	8,260	50 MB	0.5 TB
		Total	**4.5 TB**

2.3.2. Audit products (Major)

The sizing of the audit products based on assignment types is detailed below. It is important to note that the sizing per product is only approximate.

Nature of product	Number of products[2]	Sizing per product	Total sizing (Approximate)
Inspection reports	48,106	10 MB	0.5 TB
Audit reports	98	50 MB	0.05 TB
Audit certificates	8,260	10 MB	0.1 TB
		Total	**~1 TB**

[1] Based on 2017-18 data as reflected in the 2017-18 Performance Activity Report of IA&AD

[2] Based on 2017-18 data as reflected in the 2017-18 Performance Activity Report of IA&AD

Comptroller and Auditor General of India

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Request for Proposal

`Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

‘One IA&AD One System’ (OIOS) Project

VOLUME - 2

Reference Number: 51-ISW/2019-‘One IA&AD One System’ Project

Page Intentionally Left Blank

Disclaimer

The information contained in this Request for Proposal document ("RFP") or subsequently provided to Bidders, whether verbally or in documentary or any other form by or on behalf of the Comptroller & Auditor General of India (C&AG/ IA&AD), or any of its employees or advisors, is provided to the Bidders on the Terms and Conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is neither an offer nor an invitation by IA&AD to the prospective Bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in the formulation of their Proposals pursuant to this RFP.

This RFP may not be appropriate for all companies, and it is not possible for IA&AD, its employees or advisers to consider the objectives, technical expertise and particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP may not be complete, accurate, adequate or correct. Each bidder should therefore conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments and information contained in this RFP and obtain independent advice from appropriate sources.

Information provided in this RFP to the Bidders is on a wide range of matters, some of which depend upon interpretation of facts. The information given is not an exhaustive account of requirements and should not be regarded as a complete or authoritative statement of facts. The specifications laid out in this RFP are indicated as the minimum requirements whereas the bidders are expected to focus on the objectives of the project and formulate their solution offerings in a manner that enables achieving those objectives in letter as well as spirit.

IA&AD accepts no responsibility for the accuracy or otherwise for any interpretation or opinion expressed herein. IA&AD , its employees and advisors make no representation or warranty and shall have no liability to any person including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, reliability or completeness of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process.

Page Intentionally Left Blank

Glossary of Acronyms	
Acronym	Full text
AD	Active Directory
ADM	Audit Design Matrix
AMC	Annual Maintenance Contract
API	Application Program Interface
APM	Application Performance Monitoring
APT	Advanced Persistent Threat
BI	Business Intelligence
BCP	Business Continuity Planning
BPM	Business Process Management
C&AG	Comptroller and Auditor General of India
CERT-In	Indian Computer Emergency Response Team
CIN	Corporate Identification Number
CMMI	Capability Maturity Model Integration
CPU	Central Processing Unit
COTS	Commercial Off-The-Shelf product
CPP	Central Public Procurement
DC	Data Center
DMS	Document Management System
DMZ	Demilitarized zone
DR	Disaster recovery
DRC	Disaster Recovery Centre
DW	Data Warehouse
EMD	Earnest Money Deposit
EMS	Event Monitoring Service
FAO	Field Audit Office
GFR	General Financial Rules
GIS	Geographical Information System
GOI	Government of India
GST	Goods & Services Tax
GUI	Graphical User Interface

HQ	Headquarters
HR	Human Resources
HSM	Hardware Security Module
IA&AD	Indian Audit and Accounts Department; often used interchangeable with C&AG (Comptroller and Auditor General of India)
ICISA	International Centre for Information Systems and Audit
ICT	Information & Communication Technology
IEC	International Electro-technical Commission
IFMS	Integrated Financial Management System
INR	Indian Rupee
IP	Internet Protocol
IPMP	Integrated Project Management Plan
IR	Inspection Report
IS	Information System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITA	Internal Test Audit
IW	Inspection Wing
KD	Key Document
KMS	Knowledge Management System
KPI	Key Performance Indicator
LAN	Local Area Network
LB	Local Bodies
LC	Legislative Committee
LLP	Limited Liability Partnership
LOI	Letter of Intent
LTO	Linear Tape Open
MeitY	Ministry of Electronics & Information Technology
MIS	Management Information System
MPLS	Multi-Protocol Label Switching
MSA	Master Services Agreement

MZ	Militarized Zone
NAC	Network Access Control
NCR	National Capital Region
NICNET	National Informatics Centre Network
NLDC	Near Line Data Center
NLSAS	Near Line SAS
O&M	Operations and Maintenance
OEM	Original Equipment Manufacturer
OIOS	One IA&AD One System
OS	Operating System
OSC	OIOS Steering Committee
OWASP	Open Web Application Security Project
PAC	Public Accounts Committee
PAN	Permanent Account Number
PAO	Pay and Accounts Officer
PBG	Performance Bank Guarantee
PC	Personal Computer
PDC	Primary Data Centre
PECMC	Project Execution and Change Management Committee
PFMS	Public Financial Management System
PR	Peer Review
QA/QC	Quality Assurance/ Quality Control
QCBS	Quality cum Cost Based Selection
RAM	Random Access Memory
RBP	Record Based Permission
RDBMS	Relational Database Management System
RFP	Request For Proposal
ROC	Registrar of Companies
RPO	Recovery Point Objective
RTI	Right To Information Act
RTO	Recovery Time Objective

SAI	Supreme Audit Institution
SAN	Storage Area Network
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SI/IA	System Integrator/ Implementation Agency as equivalent terms
SIEM	Security information and event management
SLA	Service Level Agreement
SQL	Structure Querying Language
SSD	Solid State Device
STQC	Standardisation Testing and Quality Certification
TGS	Technical Guidance and Support
TK	Toolkit
UAT	User Acceptance Testing
UTF	Unicode Transformation Format
VAPT	Vulnerability Assessment Penetration Testing
VLAN	Virtual Local Area Network
VLC	Voucher Level Computerization
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall

Page Intentionally Left Blank

1 Table of Contents

2 RFP Issuing Authority

This RFP is issued by Comptroller and Auditor General of India, New Delhi.

I.	**Project Title**
	“ One IAAD One System (OIOS)”
II.	**RFP Issuer**
	Deputy Director (IS) Office of the Comptroller and Auditor General of India, 9, Deen Dayal Upadhyaya Marg New Delhi - 110124
III.	**Contact Person – Nodal Officer**
	Name: Sreeraj Ashok
	Phone No: 011-23235055
	Email Id: oios@cag.gov.in
IV.	Important dates: Refer section 6

3 Fact Sheet

S. No.	Clause Reference	Description
1.	RFP Vol 2 - Section 6	Tender Schedule: Important Dates
2.	RFP Volume 2 – Section 7.7.6	**Method of Selection:** The method of Selection is **Quality Cum Cost Based Selection (QCBS)**; the technical proposals would be allotted a weightage of 70% while the financial proposals will be allotted a weightage of 30%
3.	RFP Volume 2 – Section 7.4	**The RFP can be downloaded from** https://cag.gov.in and https://eprocure.gov.in/eprocure/app
4.	RFP Volume 2 – Section 7.3.3	**Earnest Money Deposit:** EMD of Rs. *25 lakhs only* in the form of Account Payee Demand Draft OR Bankers Cheque OR Bank Guarantee
5.	RFP Volume 2 – Section 6 & Section 7.2.1	**Pre Bid Meeting and Clarification** A pre-bid meeting will be held on the date as mentioned in Section 6 of this document. The name, address, and telephone numbers of the nodal officer is: **Sreeraj Ashok** **Deputy Director (IS)** **Office of the Comptroller and Auditor General of India** **9, Deen Dayal Upadhyaya Marg, New Delhi-110124** **Phone: 011-23235055** **oios@cag.gov.in** All queries should be received on or before the date as mentioned in Section 6, through email.
6.	RFP Vol 2 – Section 7.7.1	For Pre-Qualification Criteria Refer section 7.7.1 of RFP Volume 2

S. No.	Clause Reference	Description
7.	RFP Volume 2 – Section 7.5.2	**Language of Proposal :** Proposals should be submitted in English language only
8.	RFP Volume 2	**Taxes:** Taxes must be explicitly mentioned in the provided bid templates.
9.	RFP Volume – 2 Section – 7.6.2	**Proposal Validity** Proposals must remain valid till 180 days from the Bid Submission Closing Date.
10.	RFP Volume 2 – Section 7.4 & 7.5	**Submission of Proposals:** Electronic Proposal submission on https://eprocure.gov.in/eprocure/app Proposal Submission / Upload: Bidders must upload and submit on the eProcurement portal https://eprocure.gov.in/eprocure/app all the items (documents), as per the folder structure specified on the eProcurement portal. Each of the above documents must be uploaded in the format specified for this purpose.
11.	RFP Volume II – Section 6	**Proposal Submission Closing** Proposals must be submitted before as per the schedule given in Section 6 of this document. Proposals submitted after Proposal Submission Closing Date & Time shall not be accepted by the eProcurement portal
12.	RFP Vol II – Section 7.7.3	**Technical Evaluation:** For each section of the Technical Evaluation Matrix, the bidder has to score a minimum cut off marks of 45 % apart from scoring a minimum of 65% marks in aggregate to qualify Technical Evaluation.
13.	RFP Vol II - Downstream Work	IA&AD does not envisage any downstream work
14.	RFP Vol II – Section 7.2.1	Venue for Pre Bid Conference iCISA, A-52, Institutional Area, Block A, Industrial Area, Sector 62, Noida,

S. No.	Clause Reference	Description
		Uttar Pradesh 201301 **0120-2400050/52**
15.	RFP Volume I	**Scope of Work** For Detailed Scope of Work, refer RFP Volume 1

1. Proposals, in complete form in all respects as specified in the RFP, must be submitted on the portal within the date and time as specified in Section 6.

2. IA&AD may, in exceptional circumstances and at its discretion, extend the deadline for submission of proposals by issuing an addendum, in which case all rights and obligations of IA&AD and the bidders previously subject to the original deadline will thereafter be subject to the deadline as extended.

4 Request for Proposal

Tenders are invited from eligible, reputed, qualified Information Technology (IT) firms with sound technical and financial capabilities for design, development, implementation and maintenance of an end to end IT solution as detailed out in the scope of work of this RFP in Volume 1. This invitation to bid is open to all bidders meeting the minimum eligibility criteria as mentioned in Volume 2 of the RFP document.

5 Structure of the RFP

Volume 1: Functional and Technical Requirements

Volume1 of this RFP intends to bring out the details with respect to scope of work, project implementation, timelines, solution and other requirements that IA&AD deems necessary to share with the potential bidders. The information set out in this volume has been broadly categorized as Functional, Technical and Operational requirements covering multiple aspects of the requirements.

Volume 2: Bidding Terms & Conditions and Evaluation Process

Volume 2 of this RFP purports to detail out all information that may be needed by the potential bidders to understand the commercial terms and bidding process details.

Volume 3: Draft Master Service Agreement

Volume 3 of this RFP is essentially devoted to explaining the contractual terms that IA&AD wishes to specify at this stage. It consists of a draft of the Master Services Agreement (MSA), including Service Level Agreement (SLA) that needs to be signed between IA&AD and the successful bidder (IA).

Note: The bidders are expected to examine all instructions, forms, terms, Project requirements and other information in the RFP documents. Failure to furnish all information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the Bidder's risk and may result in rejection of the proposal.

This document is Volume 2 of the RFP.

6 Tender Schedule: Important Dates

S No	Particular	Details (To Be Filled)
1.	Release of Request For Proposal (RFP)	Thursday, 22-Aug-2019 10:00 AM
2.	Last date for Submission of Written Queries by Bidders	Monday, 02-Sep-2019 05:00 PM
3.	Pre-Bid Conference	Wednesday, 04-Sep-2019 11:00 AM
4.	Date of Publishing of Pre Bid Response	Friday, 06-Sep-2019 04:00 PM
5.	Proposal Submission Start Date	Friday, 20-Sep-2019 09:00 AM
6.	Proposal Submission End Date	Friday, 27-Sep-2019 06:00 PM
7.	Date & time of opening of Pre-Qualification bids	Monday, 30-Sep-2019 11:00 AM
8.	Date & time of opening of Technical bids	Will be intimated later
9.	Date & time of opening of Commercial bids	Will be intimated later

7 Instructions to Bidders

7.1 General

a) While every effort has been made to provide comprehensive and accurate background information and requirements and specifications, Bidders must form their own conclusions about the solution needed to meet the requirements. Bidders and recipients of this RFP may wish to consult their own legal advisers in relation to this RFP.

b) All information supplied by Bidders may be treated as contractually binding on the Bidders, on successful award of the assignment by IA&AD on the basis of this RFP.

c) No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of IA&AD. Any notification of preferred Bidder status by IA&AD shall not give rise to any enforceable rights by the Bidder. IA&AD may cancel this public procurement at any time prior to a formal written contract with the shortlisted bidder.

d) This RFP supersedes and replaces any previous public documentation & communications, and Bidders should place no reliance on such communications.

7.1.1 Eligibility to Bid

a) This invitation for bids is open to all Indian firms who fulfil pre-qualification criteria as specified in this Volume of RFP.

b) Bidders declared by IA&AD or Government of India to be ineligible to participate for unsatisfactory past performance, corrupt, fraudulent or any other unethical business practices shall not be eligible.

c) Breach of general or specific instructions for bidding, general and special conditions of contract with IA&AD during the past 5 years shall make a firm ineligible to participate in bidding process.

d) A company shall submit only one response to the RFP. In case of alternate/multiple responses by one bidder, both the responses shall be considered invalid.

e) Consortium is not allowed.

7.1.2 Acceptance part/ whole bid/ modification – rights thereof

IA&AD reserves the right to modify the technical specifications/ quantities/ requirements/ tenure mentioned in this RFP including addition/ deletion of any of the item or part thereof after pre-bid meeting and the right to accept or reject wholly or partly bid offer, or, without assigning any reason whatsoever. No correspondence in this regard shall be entertained. IA&AD also reserves the unconditional right to place order on wholly or partly bid quantity to the successful bidder.

7.1.3 Interlineations in Bids

Documents submitted in scanned form shall contain no interlineations, erasures or overwriting except as necessary to correct errors made by the Bidder, in which case such corrections shall be initialled by the person or persons signing the bid.

7.1.4 Conditions Under which this RFP is issued

a) This RFP is not an offer and is issued with no commitment. IA&AD reserves the right to withdraw the RFP and change or vary any part thereof at any stage.

b) Timing and sequence of events resulting from this RFP shall ultimately be determined by IA&AD.

c) No oral conversations or agreements with any official, agent, or employee of IA&AD shall affect or modify any terms of this RFP and any alleged oral agreement or arrangement made by a bidder with any IA&AD, agency, official or employee of IA&AD shall be superseded by the definitive agreement that results from this RFP process. Oral communications by IA&AD to bidders shall not be considered binding on IA&AD, nor shall any written materials provided by any person other than IA&AD.

d) Neither the bidder nor any of the bidder's representatives shall have any claims whatsoever against IA&AD or any of their respective officials, agents, or employees arising out of, or relating to this RFP or these procedures (other than those arising under a definitive service agreement with the bidder) in accordance with the terms thereof.

e) All bidders, until the contract is awarded and the successful bidder, during the currency of the contract shall not, directly or indirectly, solicit any employee of IA&AD or any other officials involved in this RFP process in order to accept employment with the organization, or any person acting in concert with the bidder, without prior written approval of IA&AD.

7.1.5 Rights to the Content of the Proposal

a) All the bids and accompanying documentation submitted as bids against this RFP will become the property of IA&AD.

b) IA&AD is not restricted in its rights to use or disclose any or all of the information contained in the proposal and can do so without compensation to the bidders.

c) IA&AD shall not be bound by any language in the proposal indicating the confidentiality of the proposal or any other restriction on its use or disclosure.

d) IA&AD has the right to use the services of external experts to evaluate the proposal by the bidders and share the content of the proposal either partially or completely with the experts for evaluation.

7.1.6 Acknowledgment of Understanding of Terms

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

7.1.7 Confidentiality

Information relating to the examination, clarification, comparison and evaluation of the bids submitted shall not be disclosed to any of the responding firms or their representatives or to any other persons not officially concerned with such process until the selection process is over. The undue use by any responding firm of confidential information related to the process may result in rejection of its bid.

7.1.8 Publicity

Bidder shall not perform any kind of promotion, publicity or advertising etc. at IA&AD and their field offices through any kinds of hoardings, banners or the like without the prior written consent of the IA&AD.

7.1.9 Government Regulations

a) In order to discharge the obligations in respect of supply of products and services, it is essential that the SI / OEMs confirm that there are no Government restrictions or limitations in the country of the supplier or countries from which subcomponents are being procured and / or for the export of any part of the system being supplied.

b) SI, OEM should further confirm that products/ services are not put to use in India where there are government regulations which prohibit use of such products / services for hosting government applications or sensitive government data.

7.1.10 Compliant Proposals / Completeness of Response

a) Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

b) Failure to comply with the requirements of this paragraph may render the Proposal non- compliant and the Proposal may be rejected. Bidders must:

I. Include all documentation specified in this RFP;

II. Follow the format of this RFP and respond to each element in the order as set out in this RFP

III. Comply with all requirements as set out within this RFP.

7.1.11 Code of integrity

No official of IA&AD or a bidder shall act in contravention of the codes which includes

a. Prohibition of

i. Making offer, solicitation or acceptance of bribe, reward or gift or any material benefit, either directly or indirectly, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process.

ii. Any omission, or misrepresentation that may mislead or attempt to mislead so that financial or other benefit may be obtained or an obligation avoided.

iii. Any collusion, bid rigging or anticompetitive behaviour that may impair the transparency, fairness and the progress of the procurement process.

iv. Improper use of information provided by the procuring entity to the bidder with an intent to gain unfair advantage in the procurement process or for personal gain.

v. Any financial or business transactions between the bidder and any official of the procuring entity related to tender or execution process of contract, which can affect the decision of the procuring entity directly or indirectly.

vi. Any coercion or any threat to impair or harm, directly or indirectly, any party or its property to influence the procurement process.

vii. Obstruction of any investigation or auditing of a procurement process

viii. Making false declaration or providing false information for participation in a tender process or to secure a contract;

b. Disclosure of conflict of interest

Disclosure by the bidder of any previous transgressions made in respect of the provisions of sub-clause (a) with any entity in any country during the last three years or of being debarred by any other procuring entity.

In case of any reported violations, if IA&AD, after giving a reasonable opportunity of being heard, comes to the conclusion that a bidder or prospective bidder, as the case may be, has contravened the code of integrity, it will take appropriate measures.

7.2 Pre-Bid Meeting & Clarifications

7.2.1 Pre-bid Conference

a. IA&AD shall hold a pre-bid meeting with the prospective Bidders on the date as specified in Section 6: Tender Schedule: Important Dates at the address as mentioned in Section 3 Fact Sheet.

b. The Bidders will have to ensure that their queries for pre-bid meeting should reach the contact person through email on or before the date and time as mentioned in the Section 6; Tender Schedule: Important Dates to the Contact person as mentioned in the Section 2. RFP Issuing Authority, line item III – Contact Person. The email id and address are mentioned there

c. The queries should necessarily be submitted in the following format:

S. No.	RFP document reference(s) (RFP Vol , Section & page number)	Content of RFP requiring clarification(s)	Observation/ Suggestion	Type of observation (Compliance issue, suggestion)	Justification

Note: Bidder may submit query in a spreadsheet.

d. IA&AD shall not be responsible for ensuring that the Bidders' queries have been received by it. Any requests for clarifications post the indicated date and time may not be entertained by IA&AD.

7.2.2 Responses to Pre-Bid Queries and Issue of Corrigendum

a. The Nodal Officer notified by IA&AD will endeavour to provide timely response to all queries. However, IA&AD makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does IA&AD undertake to answer all the queries that have been posed by the Bidders.

b. At any time prior to the last date for receipt of bids, IA&AD may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP Document by a corrigendum.

c. The corrigendum (if any) & clarifications to the queries from all Bidders will be posted on https://cag.gov.in, https://eprocure.gov.in/eprocure/app and may be emailed to all participants of the pre-bid conference.

d. Any such corrigendum shall be deemed to be incorporated into this RFP.

e. In order to provide prospective Bidders reasonable time for taking the corrigendum into account, IA&AD may, at its discretion, extend the last date for the receipt of Proposals

7.3 Key instructions of the bid

7.3.1 Right to Terminate the Process

a. IA&AD may terminate the RFP process at any time and without assigning any reason. IA&AD makes no commitments, express or implied, that this process will result in a business transaction with anyone.

b. This RFP does not constitute an offer by IA&AD. The Bidder's participation in this process may result

IA&AD selecting the Bidder to engage towards execution of the subsequent contract.

7.3.2 RFP document fees

The RFP documents have been made available for download without any fee from the websites as mentioned in the Factsheet.

7.3.3 Earnest Money Deposit (EMD)/ Bid Security

1. Bidders shall submit, along with their Proposals, an EMD of Rs. 25,00,000 (25 Lakhs) only, in the form of a Demand Draft OR Bankers Cheque OR Bank Guarantee under the payment related information:

    i. EMD BG in the format specified in Appendix I: Form 3 issued by a commercial bank in favour of **PAO, Office of the Comptroller and Auditor General of India, payable at New Delhi**. The EMD BG should remain valid for a period of 45 days beyond the proposal validity period.

    ii. Demand Draft/Banker cheque : Payable in favour of PAO, Office of the Comptroller and Auditor General, payable at New Delhi

2. EMD of all unsuccessful Bidders would be refunded by IA&AD within 45 days of the Bidder being notified as being unsuccessful. The EMD, for the amount mentioned above, of the successful Bidder would be returned upon submission of Performance Bank Guarantee as per the Format 1 provided in Appendix III.

3. The EMD amount is interest free and will be refundable to the unsuccessful Bidders without any accrued interest on it.

4. Proposals not accompanied by the EMD or containing EMD with infirmity (ies) (relating to the amount or validity period etc.), mentioned above, shall be summarily rejected.

5. The EMD may be forfeited in the event of:

    i. A Bidder withdrawing its bid during the period of bid validity or any extension agreed by the bidder thereof

    ii. If the bid is varied or modified in a manner not acceptable to IA&AD after opening of Bid during the validity period or any extension thereof.

    iii. If the Bidder withdraws its bid during evaluation.

    iv. A successful Bidder fails to sign the subsequent contract in accordance with this RFP

v. If the Bidder, having been notified of his selection, fails or refuses to submit the required Performance Bank Guarantee within the time stipulated by IA&AD

vi. The Bidder being found to have indulged in any suppression of facts, furnishing of fraudulent statement, misconduct, or other dishonest or other ethically improper activity, in relation to this RFP.

7.4 Submission of Proposals

7.4.1 Online Submission on e-Procurement Portal

IA&AD invites proposals from the qualified bidders on the Electronic Tender Platform as mentioned in the fact sheet. The bidders are required to submit soft copies of their bids electronically, duly signed using Digital Signature Certificates, on the e-tendering platform.

Bidders should submit their responses as per the procedure specified in the e-Procurement portal (https://eprocure.gov.in/eprocure/app) being used for this purpose.

The documents must be uploaded in the format specified for this purpose and as per the specified folder structure in the e-Procurement portal.

The bidder must ensure that the bid is digitally signed by the Authorized Signatory of the bidding firm and has been duly submitted (freezed) within the submission timelines. IA&AD will in no case be responsible if the bid is not submitted online within the specified timelines.

All the pages of the Proposal document must be sequentially numbered and must contain the list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bidder’s Proposal.

Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority or the relevant contact person indicated in the RFP document within the specified timelines.

Bidder instructions and user guide are available on the Homepage of the e-tendering platform under the link as mentioned in the fact sheet. Bidders are requested to go through the instructions and user guide in advance. In case of any queries relating to the Bid preparation and submission on e-tendering platform, Bidder can contact the e-tendering platform helpdesk.

i. The Bid shall be typed in English and digitally signed by the Bidder or a person duly authorized to bind the Bidder to the Contract.

ii. All the documents uploaded in the bid envelopes must be digitally signed by the authorized representative.

iii. Power-of-attorney Document (in the name of the signatory of the proposal) must be printed on Company letter head and ink signed. It should be scanned & uploaded in the Pre-Q envelope.

iv. It is mandatory for the Bidder to quote for all the items mentioned in the RFP.

v. Standard Commercial Bid Formats have been provided with the tender document to be filled in by all the bidders. Bidders are requested to note that they should necessarily submit their Commercial bids in the format provided and no other format is acceptable. If the Commercial bid file format is found to be modified by the bidder, the bid may be rejected. Templates of Technical Bid and Commercial Bid in editable format (.docx) can be downloaded with the RFP Document from the e-procurement portal.

vi. It is mandatory to provide the Masked/ Unpriced Commercial Bid along with the Technical Bid in the same format provided for in the commercial bid. The Bidder shall ensure that all line items have been carefully checked and none has been left blank. In the event that due to error or oversight (a) the Bidder has mentioned a component as part of the Masked Commercial Bid but either the line item or the price value for the same component has been left blank in the Commercial Bid, the Bidder shall be required to provide the same component to IA&AD, in the quantity mentioned in the Masked Commercial Bid, at no commercial impact to the purchaser; (b) If the quantity for the same component has been shown lower in the Commercial Bid than in the Masked Commercial Bid, the Bidder shall be required to provide the same component in the quantity mentioned in the Masked Commercial Bid.

vii. The server time will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc.

viii. All the documents being submitted by the bidders would be encrypted by IA&AD’s private key through the e-tendering platform.

ix. All bidders must fill Electronic Forms (if applicable) for each bid-part sincerely and carefully and avoid any discrepancy between information given in the Electronic Forms and the corresponding

Main Bid/documents uploaded. If any variation is noted between the information contained in the Electronic Forms and Main Bid/documents uploaded, the content of the Main Bid/documents shall prevail.

x. Upon the successful and timely submission of bids, the portal will give a successful bid submission message & **a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details**. Bidders are advised to take printout of the bid summary and the bid receipt and keep it safe for record purpose.

xi. Prices should not be indicated in the Pre-Qualification Proposal or Technical Proposal or the Masked Commercial Bid/ Unpriced Bid accompanying the Technical Proposal but should only be indicated in the Commercial Proposal.

xii. Commercial Bid sheets must be uploaded in Excel Format.

xiii. Bidders are advised to study this RFP document carefully before submitting their Pre-qualification, Technical and Commercial bids in response to the bid Invitation.

xiv. IA&AD will not accept delivery of proposal in any manner other than that specified above.

xv. If any bidder does not qualify in the prequalification evaluation, the technical and commercial proposals shall not be opened.

xvi. If any bidder does not qualify in the technical evaluation, the commercial proposal shall not be opened.

xvii. IA&AD will not accept delivery of proposals by Post or Email. Such proposals shall be rejected.

7.4.2 Bidder’s authorised Signatory

A Proposal should be accompanied by an appropriate board resolution or power of attorney in the name of an authorized signatory of the Bidder stating that he is authorized to execute documents and to undertake any activity associated with the Bidder’s Proposal. Power of attorney should be on the company letter head. A copy of the same should be uploaded under the relevant section/folder on the e-Procurement portal. Furthermore, the bid must also be submitted online after being digitally signed by an authorized representative of the bidding entity.

7.5 Preparation and submission of Proposals

7.5.1 Proposal preparation costs

The Bidder shall be responsible for all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposals, in providing any additional information required by IA&AD to facilitate the evaluation process, and in negotiating a definitive contract, or all such activities related to the bid process.

IA&AD will in no event be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

7.5.2 Language of the bid

The Proposal should be filled by the Bidder in the English language only. If any supporting documents submitted are in any language other than English, translation of the same in the English language is to be duly attested by the Bidders. For purposes of Proposal evaluation, the English translation shall prevail.

7.5.3 Venue & Deadline for Submission of Proposals

The response to RFPs must be submitted on the eProcurement portal by the date and time specified for the RFP and mentioned in RFP Vol II, Section 3 Fact Sheet. Any proposal submitted on the portal after the above deadline will not be accepted and hence shall be automatically rejected. IA&AD shall not be responsible for any delay in the submission of the documents.

7.5.4 Proposals submitted after designated time of submission

Bids submitted after the due date will not be accepted by the e-Procurement portal and hence will automatically be rejected. IA&AD shall not be responsible for any delay in the online submission of the proposal and no correspondence in this regard will be entertained.

7.6 Evaluation Process

a. IA&AD will constitute a committee to evaluate the responses of the Bidders (Purchase Committee).

b. The Purchase Committee constituted by IA&AD shall evaluate the responses to the RFP and all supporting documents / documentary evidence. Inability of a Bidder to submit requisite supporting documents / documentary evidence within a reasonable time (as determined by IA&AD) provided to it, may lead to the Bidder's Proposal being declared non-responsive.

c. The decision of the Purchase Committee in the evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of negotiation/ discussion with the Purchase Committee.

d. The Purchase Committee may ask for meetings with the Bidders to seek clarifications on their proposals.

e. The Purchase Committee reserves the right to reject any or all Proposals on the basis of any deviations contained in them.

f. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.

7.6.1 Proposal opening

The Proposals submitted as per schedule provided in RFP Vol 2, Section 6 – Tender Schedule: Important Dates or any revisions will be opened as per the date and time as mentioned in the said section or any revisions thereof by the Nodal Officer or any other officer authorized by IA&AD, in the presence of the Bidder's representatives who may be present at the time of opening.

The representatives of the Bidders shall carry an identity card or a letter of authority from the Bidding entity to identify their bona fides for attending the opening of the Proposal.

7.6.2 Proposal validity

The offer submitted by the Bidders should be valid for minimum period of 180 days from the date of Bid Submission Closing.

a) A bid valid for a shorter period shall be rejected by IA&AD as non-responsive.

b) In exceptional circumstances, IA&AD may solicit the bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing (by email). The EMD/ bid security validity shall also be suitably extended. A bidder may refuse the request without forfeiting his bid security. A bidder granting the request shall not be permitted to modify his bid.

7.6.3 Proposal evaluation

a. Initial Proposal scrutiny will be held to confirm that Proposals do not suffer from the infirmities detailed below. Proposals will be treated as non-responsive, if a Proposal is found to have been:

    i. submitted in a manner not conforming with the manner specified in the RFP document

    ii. submitted without appropriate EMD as prescribed herein

- iii. received without the appropriate or power of attorney
- iv. containing subjective/incomplete information
- v. submitted without the documents requested in the checklist
- vi. non-compliant with any of the clauses stipulated in the RFP
- vii. having lesser than the prescribed validity period.

The EMD of all non-responsive bids shall be returned to the bidders as quoted in earlier section of this RFP.

b. All responsive Bids will be considered for further processing as below.

IA&AD will prepare a list of responsive Bidders, who comply with all the Terms and Conditions of the Tender. All eligible bids will be considered for further evaluation by a Committee according to the Evaluation process defined in this RFP document. The decision of the Committee will be final in this regard.

7.7 Criteria for evaluation

7.7.1 Pre-qualification (PQ) criteria

S No	Basic Requirement	Specific Requirement	Documents Required
1.	EMD	Bidder must submit EMD of Rs. 25 Lakhs to IA&AD as per RFP/tender format	Demand Draft (DD) or Bankers Cheque or Bank Guarantee
2.	Power of Attorney	Board resolution or power of attorney in the name of an Authorized Signatory of the Bidder stating that he is authorized to execute documents and to undertake any activity associated with the Bidder's Proposal	Notarised copy of Board Resolution or Power of Attorney in the name of the Authorized signatory
3.	Legal Entity	The following Indian Firms are allowed to participate in the bid process: I. Companies registered under Companies Act 1956 or 2013 II. Partnership firms registered under Limited Liability Partnerships (registered under LLP Act, 2008)	Certificate of Incorporation Registration Certificates (Copy of the certificate to be legible showing the CIN number clearly)

S No	Basic Requirement	Specific Requirement	Documents Required
		III. Partnership firms registered under Indian Partnership Act, 1932	
4.	Statutory Tax Registrations	The Bidder should have: (i) Valid PAN Number (ii) Valid GST Number	Copy of PAN Card Copy of GST Registration Certificate
5.	Sales turnover from IT Consultancy/ IT Advisory Services	The Bidder should have an annual turnover of not less than INR 1500 **Crores p.a.** in each of three financial years (F.Y. 2015-16, 2016-17, 2017-18 respectively). This turnover should be on account of IT Consultancy/ IT Advisory Services only. The turnover refers to the turnover of the company and not the composite turnover of its subsidiaries/sister concerns, etc.	Extracts from the audited balance sheet and profit & loss OR Certificate from the statutory auditor or a Chartered Accountant. In case revenues from IT Consultancy/ IT Advisory Services are not separately mentioned in the audit reports, a Certificate from the bidder's statutory auditor/Company Secretary shall be provided, specifying the relevant turnover for the respective years.
6.	Net worth Requirements	The Bidder should have positive net worth in each of three financial years i.e., (F.Y. 2015-16, 2016-17 and 2017-18 respectively)	Company Secretaries or a Chartered Accountant's Certificate mentioning Net-Worth
7.	Certifications	The Bidder should have : (i) Valid CMMI Level 5	Copy of Certificates

S No	Basic Requirement	Specific Requirement	Documents Required
		(ii) ISO 27001 The certifications should be valid on the date of bid submission. In case of Service Providers where the CMMI certification is under renewal, the Bidder shall provide the details of the previous CMMI certification and the current assessment details for consideration in the Bid Process. Further, if the Bidder is selected, it shall ensure that the certifications continue to remain valid till the end of the Agreement.	• Maturity level 5(Optimizing) – CMMI Dev Version 1.3 Certificate • ISO 27001 Certificate
8.	Blacklisting and Debarment	The Bidder shall not be under a declaration of ineligibility / banned / blacklisted by the Central Government/PSU any other Central Government institutions in India for any reason as on the last date of submission of the Bid or convicted of economic offence in India for any reason as on the last date of submission of the Bid. AND The Bidder should have not been convicted/ debarred ▪ Under the Prevention of Corruption Act, 1988; OR ▪ The Indian Penal Code OR ▪ Any other law for the time being in force, for causing any loss of life or property or causing a threat to public health as part of	A Self Certified letter

S No	Basic Requirement	Specific Requirement	Documents Required
		execution of a public procurement contract. ▪ The Bidder should not have been under the debarred list as per GFR 2017, Rule 151	
9.	Technical Capacity	The Bidder should be an IT-solutions-provider incorporated in India and should have successfully implemented project(s) in the last five financial years as below: i. One System Integration / e-Governance project of minimum – INR 60 Crore or ii. Two System Integration / e-Governance projects of minimum – INR 45 Crores each or iii. Three System Integration / e-Governance projects of minimum – INR 30 Crores each	Copy of work order / client certificates. Completion certificates from the client; OR Work order + Self certificate of completion with details
10.	Experience in Data Center	The bidder should have Completed/on-going at least One Data Center Setup & Commissioning Project in India in the last five financial years. **Project Scope must have:** 1.Hardware/System software/Network components supply 2. Data Center Commissioning & Operations 3. Training service 4. Operation and maintenance services	Copy of work order / client certificates. Completion certificates from the client; OR Work order + Self certificate of completion with details

S No	Basic Requirement	Specific Requirement	Documents Required
		Project Value should be: - One project of not less than 20 Cr OR - Two projects each of not less than 10 Cr OR - Three or more projects each of not less than 7 Cr **On Going Projects:** Project should be Live and in Operations and Maintenance phase. Note: Supply of PC, Laptop, Printers, non-DC accessory components shall not be counted for Project value.	
11.	Manpower Strength	The bidder must have at least 1000 qualified Software Engineers on the company's payroll	Self-Certification by the authorized signatory

Only Project Citations completed/started in the last five financial years (2014-2019) will be considered for Assessment.

7.7.2 Technical Qualification Criteria

Bidders who meet the pre-qualifications/eligibility requirements as on the last date of bid submission would be considered as qualified to move to the next stage of Technical and Financial evaluations.

7.7.3 Technical Scoring Model

The following table provides the scoring model, including the cut-off marks based on which the technical bids shall be evaluated for the Implementation of OIOS Project. For each section of the Technical Evaluation Matrix, the bidder has to score a minimum cut off marks of 45 % apart from scoring a minimum of 65% marks in aggregate.

The Masked Commercial Bid/ Unpriced Commercial Bid will be used by the Evaluation Committee to support the Technical Evaluation, as necessary.

Bidders are required to furnish data with supporting documents in the prescribed format mentioned in the below mentioned table for evaluation.

Technical Evaluation Model

For each section of the Technical Evaluation Matrix, the bidder has to score a minimum of 45% marks allotted for that section apart from scoring a minimum of 65 % marks in aggregate. In case, the bidder fails to score less than 45% of marks in any of the sections, the technical proposal of that bidder would be rejected and therefore the bidder's commercial quote shall not be opened.

Sec. No	**Sec. Name**	**Section Evaluation Parameters**	**Max Marks (Tn)**	**Supporting Docs/ Bid Reference**
S.1	**Proposal on OIOS Application Functionality**		**22**	Compliance Note
		Meeting the requirements of OIOS Application in terms of how close the proposal is to the functional requirements for the solution as have been proposed for IA&AD.	Detailed breakup provided in subsequent tables	
Row Intentionally left blank				
S.2	**Technologies proposed for OIOS Application**		**25**	Note
		Demonstrated robustness of the technology deployed across other installations around India, including – Scalability – Security – Ease of implementation	Detailed breakup provided in subsequent tables	
S.3	**Project Methodology, Support and Documentation**		**15**	Note
		Qualitative assessment based on – **Understanding of the objectives of the assignment:** The extent to which the Systems Implementer's approach and work plan respond to the objectives indicated in the Statement/Scope of Work – **Completeness and responsiveness:** The extent to which the proposal responds exhaustively to all the requirements of the RFP	Detailed breakup provided in subsequent tables	
Row Intentionally left blank				
S.4	**Training Plan**		**5**	Note
		a) Training plan & structure b) Training methodology *c)* Innovation in Training to facilitate learning experience	As per details given in the subsequent section	

Technical Evaluation Model

For each section of the Technical Evaluation Matrix, the bidder has to score a minimum of 45% marks allotted for that section apart from scoring a minimum of 65 % marks in aggregate. In case, the bidder fails to score less than 45% of marks in any of the sections, the technical proposal of that bidder would be rejected and therefore the bidder's commercial quote shall not be opened.

Sec. No	Sec. Name	Section Evaluation Parameters	Max Marks (Tn)	Supporting Docs/ Bid Reference
Row Intentionally left blank				
S.5	**Profile of proposed team members**		**10**	CVs
		Profiles of Key Personnel submitted by the bidder	Detailed breakup provided in subsequent tables	
Row Intentionally left blank				
S.6	**Exit Management**		**8**	Note and Illustrative Checklist(s)
		Clear and concise Exit Management Plan: Please provide an Illustrative exit management & transition checklist used by SI in any previous project. SI shall also separately indicate the exit management and transition checklist used for moving from one CSP to another or to on-premises DC/ DR solution or vice versa. (SI may mask relevant fields, as they wish)		
Row Intentionally left blank				
S.7	**Technical Presentation and Client Visit/ Client Interaction**		**15**	Presentation/ Interaction
		a) Presentation on understanding of the OIOS requirements & Technical Proposal, and Interaction with Key Personnel proposed by Bidder b) Client site visit/ Client interaction (Bidder shall propose three Client Site Visits or Client Interactions within India; the clients should be for projects completed/ started in the last five financial years. The Evaluation Committee shall be free	Please see details in the following section	

Technical Evaluation Model				
For each section of the Technical Evaluation Matrix, the bidder has to score a minimum of 45% marks allotted for that section apart from scoring a minimum of 65 % marks in aggregate. In case, the bidder fails to score less than 45% of marks in any of the sections, the technical proposal of that bidder would be rejected and therefore the bidder's commercial quote shall not be opened.				
Sec. No	**Sec. Name**	**Section Evaluation Parameters**	**Max Marks (Tn)**	**Supporting Docs/ Bid Reference**
		to choose one or more of the proposed references for its Client Visit/ Client Interaction.)		
	Total Marks		**100**	

OIOS Application Functionality

The responses by Bidders would be reviewed for the following aspects of the proposed OIOS solution:

- Configurability, scalability, ease of use and features & functionalities of the various functional modules of OIOS

Bidder furnishing comprehensive information closest to IA&AD's expectations as listed in this RFP shall be awarded the maximum points.

Evaluation Criterion	Benchmark / Preferences	Max Marks
Application Configurability and Scalability across IA&AD	How do you have an Enterprise wide solution running across multiple streams and multiple audit offices yet maintaining both a common core of mandatory functionality and configurability: a. How will the solution & implementation approach scale and validate configurability once moving from 5 pilot offices to another 26 nodal offices (total 31 offices). b. How can configurability be handled using a GUI/wizard approach (i.e. not requiring change management support from SI) c. Configurability is expected but not limited in the following situations at minimum:	15

Evaluation Criterion	Benchmark / Preferences	Max Marks
	i. Configuration of Additional Data elements (including Master Data) for Auditee Universe ii. Configuration of Organization Structure in different offices, therefore implementing role based access iii. Configuration of workflow depending on office or audit product or other functional needs iv. Configuration of templates for Audit Requisitions, Audit Observations and various types of Audit Products. d. The application is expected to be in use minimum for a decade. How will the OIOS Application Architecture minimise the requirement for change management by SI, while allowing configurability by the IA&AD Application Administrator?	
Empowering IA&AD personnel	How will the solution empower: a. Field Audit Teams b. Everybody else up the IA&AD hierarchy including the management	6
Offline online functionality	Audit teams go on field visits to areas where sometimes internet connectivity is unreliable or poor or in rare cases non-existent. Nevertheless, we want a solution which is a centrally controlled solution. How can the solution implement offline functionality as a back up in situations like following: a. The audit team should be able to access reference documents from KMS, specific to the assignment they are going. b. The audit team should be able to generate, even if internet connectivity goes down, Audit Requisitions and Audit Observations based on their study of paper based documentation provided by the auditable entity.	8

Evaluation Criterion	Benchmark / Preferences	Max Marks
	c. The audit team may take supporting documentation either on paper or scan limited documentation using their mobile phones or a combination thereof. d. Later on when internet connectivity is available, the work done should be synchronized automatically, with resolution of documents conflict if any. The audit team should be able to add or amend references to the supporting documents, upload supporting documentation not already uploaded etc. e. How can all this be achieved while still maintaining single source of truth at centralised Enterprise level application?	
Data Collection Kit	How would you provide a configurable platform by which the audit team can create or reuse an Audit toolkit for collecting data / findings for an audit assignment? a. How can this platform be reusable for adhoc data collection and consolidation for multiple uses? b. How can this platform be used for consolidation by multiple teams working under the same assignment? c. How this platform can work for multiple devices (laptops/desktops & mobile phones)?	8
Key supporting components	How will the solution meet our requirements for supporting documentation to be digitally available, easily linked / referenceable at different stages of the audit process. a. How can supporting documentation be reused as the audit observations move up the product hierarchy towards the C&AG's Audit Report?	8

Evaluation Criterion	Benchmark / Preferences	Max Marks
	b. How will scanning of documents by audit teams using mobile phones and uploading of documents and photographic evidences to OIOS?	
Ease of use	How will the solution handle on-boarding of users who vary widely in respect of use and knowledge of IT including simple office automation?	5
	Total	**50**

Technology

The responses by Bidders would be reviewed for the following technology aspects of the proposed solution:

- Specifications (platform, software, database design, etc.)
- Security and Scalability:
- Ease of Implementation

Also information can be collected from Vendor references (other clients for which solutions were implemented). Bidder furnishing comprehensive information closest to IA&AD's expectations as listed in the RFP shall be awarded the maximum points.

Overall Scoring (rounded to two decimal places) would be on a 25 – Point Scale.

Please refer to the following table for Scoring Template.

Evaluation Criterion	Benchmark / Preferences	Max Marks
1.Architecture		
Technology	Justification on the suggested Technology architecture with rationale and benefits. As a Best practice, and considering the scalability of the solution, a Distributed Component Architecture is preferred. In case the Bidder suggests a different architecture, the assessment would be made on the justification and reasoning provided	5

Evaluation Criterion	Benchmark / Preferences	Max Marks
2.Security		
Security Architecture	Justification on the suggested Security architecture with rationale and benefits.	3
Identification Data Integrity Data Encryption Data Confidentiality Auditability	a) Description of 2 factor/ better user authentication procedure for the proposed application b) Details on Access Controls and Privileges through application c) Encrypted storage of Username and Passwords d) Details on restriction of access to data content in the database for Users including privileged users at OS, Supporting Software (RDBMS, DMS, etc.) level	8
SIEM, Anti APT	Description of SIEM, Anti APT solution in the proposed solution	8
Firewalls and security supported by the system	Description of firewalls (Gateway, WAF) and security components (such as intrusion Prevention systems) in the proposed solution	
Data leakage prevention	Description of Data leakage prevention measures at OS, RDBMs, DMS level	
HSM	HSM sizing and solution for OIOS on Appliance/ Pay as you go model	3
3. OIOS Application Performance for the proposed solution		
Associated average response times, Concurrency for the proposed solution	a) Database update response time	3
	b) Database retrieval response time	3
Benchmark studies on technology components	Availability of Graphs, Tables, Whitepapers and related statistics of benchmarked studies on performance:	

Evaluation Criterion	Benchmark / Preferences	Max Marks
	a) Application server b) Database server c) DMS d) Reporting & BI/ Dashboard e) BPM Workflow/ Rules engine f) GIS Tool	4
6.Database/ Directory Support		
Databases **Product information (PostgreSQL/ MySQL/ MS / Oracle/ DB2, etc.)**	Relational databases which are being supported adequately in present day context would carry max score (Hierarchical / flat files databases – low score) Information on the Database products with recommendation, rationale and Enterprise level Support	6
Directory Services	Information on system support to Directory Services (LDAP data at NIC). No AD for user authentication in the proposed solution	3
7. Data Architecture		
Logical and/or physical data model.	Approach to data models with an example based on the functional specs	6
Control features for data integrity	Details on Control features to ensure data integrity such as updates, totals, cross-checks, validations etc.	3
Transaction management system	Details of transaction management at Application Level.	3
8. System management		
Rollback, recovery, and fault tolerance	Description of database failover, rollback, recovery provisions, fault tolerance at Application Level.	3

Evaluation Criterion	Benchmark / Preferences	Max Marks
System management tools	Details on provision of accepted system management tools and utilities, with appropriate notification features for effective system administration.	2
Accessibility of system management interfaces.	Details on accessibility of system management interfaces and provision for remote administration.	2
9.Web Server	Proposed Solution running on Web Server that is established and well known would be preferred (similar)	4
10. Application Server Support	Proposed Solution running on Application Server that is established and well known would be preferred (similar)	4
12.Presentation requirements		
Browsers support	Cross-browser support would be preferred (eg. IE /Mozilla/Chrome). Backward compatibility support for browser versions running on Windows 7 32-bit OS onwards. Browsers on Linux and Mac OS should also be supported.	4
Embedded browser languages	Accepted scripting language within the boundaries of sand-box. Client side Active-X controls would not be preferred.	
13. Session Management		
Concurrent users, multiple sessions	Description on handling of concurrent users, multiple sessions, session cookies.	4
System's policy on session time-outs.	Policy details on session time-outs	
14. Integration Capabilities		

Evaluation Criterion	Benchmark / Preferences	Max Marks
Integration capabilities with external, third party applications	– Elaborate on the integration methodology between modules of OIOS – Elaborate on capabilities of the solution for external integration with other applications Using Open API.	6
15. Auditing / Reporting		
Log files	Complete audit trails and log filing features of the OIOS solution, other products	8
Log files customization	a) Ability of the log files to be customized and scheduled; b) Access rights to view log files	
Querying capabilities	Details of querying capabilities, and user-friendliness of the user logs	
Procedure of audit trails	Procedure of audit, reporting and review of the proposed solution	
Compatibility with proposed monitoring tool	Demonstrate capability to integrate with offered SIEM, EMS (APM) monitoring tool	
16. Disaster Recovery and Back-up		
Disaster recovery procedures	Description of the disaster recovery procedures for data, application and client. Details of the procedure address adequate scenarios and the actions thereof	6
Archival policy	Details of archival policy and procedure for the proposed solutions. Higher the degree of automatic features / scheduling in the archival procedures, more would be score	
17. General		

Evaluation Criterion	Benchmark / Preferences	Max Marks
Any limitations in the software/operating system/file manager	Description of the limits in terms of number of table entries, database size would be assessed	5
Interdependencies in the components	Details of the interdependencies across components and possible implementation constraints would be assessed.	
Import / export facilities	Provision of import / export utilities especially to facilitate data entry / report generation	
	Total	**111**

Based on bidder's Response, score shall be assigned to each line item detailed in the table above. The total score of the bidder shall be converted to a 25-Point Scale (rounded to two decimal places)

Project Methodology, Support and Documentation

Overall Scoring would be on a 15 – Point Scale (rounded upto 2 decimal places).

Evaluation Criterion	Benchmark / Preferences	Max Marks
Project Methodology	a. Software Development Methodology using accepted standards; evaluation would be based on the rationale and clarity furnished in the bidder's response for Project Phases b. SI may explain: o Experience in using the proposed methodology, Advantages, challenges faced in previous projects and how they resolved it o Documentation standards that will be followed for OIOS project o QA & QC code review and testing approach o Approach to Definition of Done, given the IA&AD's proposed acceptance strategy (multiple levels).	20

Evaluation Criterion	Benchmark / Preferences	Max Marks
	Note: RFP does not prescribe any particular flavour of Agile Methodology. Bidder needs to provide details of proposed Agile methodology including DevOps & Agile Toolchain including details of Agile experience especially in client projects involving services and not Products.	
Support	For Phase-I, Phase-II, Phase-III a) Problem reporting and resolution mechanism b) Hotline Support c) Simultaneous Support of various releases d) Handling Change Requests e) Details of User Discussion Forum (s) f) Escalation Mechanism g) Future Upgrades	15
Operations, Security & Maintenance Plan	a) Centralized Helpdesk / proposed e-Ticketing tool b) O&M Roadmap c) Security Operations	15
	Total	50

Based on bidder’s Response, score shall be assigned to each line item detailed in the table above. The total score of bidder shall be converted to 15-Point Scale

Profile of Proposed Team Members:

The key parameters for evaluating the team members would be:

- Team Composition
- Years of Experience (of which relevant experience would be considered for evaluation)
- Qualification
- Certifications

Overall Scoring would be on a 10 – Point Scale.

Please refer to the following table for line-wise breakup

Evaluation Criterion	Benchmark / Preferences	Max Marks
Overall Project Team Structure	Composition of the Project Team Structure proposed by Bidder a) Appropriate Number of Team members with justification b) Roles and Responsibilities clearly and well defined	10
Total Years of Professional Experience	1. Project Manager to have 16+ years of total experience 2. Scrum of Scrum/ equivalent to have 12+ years of experience 3. Enterprise Solution Architect (12+ years' experience) 4. Business analysts (8+ years of experience) 5. Database Administrator to have 6+ years of experience 6. Security Architect (12+ years' experience) 7. Test lead (8+ years' experience) Note: RFP does not prescribe any particular Agile Methodology. If the Agile Methodology proposed by the bidder is other than scrum, then the equivalent designations/ specifications and Agile specific qualifications will be considered.	4 4 2 4 2 2 2
Total Years of Experience in development Projects using Agile methodology	1. Project Manager (5+ years of experience) 2. Scrum of Scrum/ equivalent (5+ years of experience) 3. Enterprise Solution Architect (5+ years' experience) 4. Business analyst (3+ years of experience) 5. Test Lead (3+ years of experience) (Note: CV of the resources shall explicitly demonstrate experience in Agile methodology)	4 4 3 4 2

Evaluation Criterion	Benchmark / Preferences	Max Marks
Certifications	a) Project Management for Project Manager & Agile Certification for key personnel b) Technology Specific certification for Key personnel	3 3
	Total	**53**

Note:

- **Key resources shall attend the Presentation during Technical evaluation. In case some of the resources are unable to attend, justification and request for VC may be made for IA&AD approval.**

Based on the bidder’s Response, a score shall be assigned to each line item detailed in the table above. The total score of the bidder shall be converted to a 10-Point Scale

- Example:

  If the Bidder Total is 40 out of the Total Score 53, on a 10-Point Scale the Score would be 40/53 * 10 = 7.55 (rounded upto 2 decimal places).

Training Plan:

The responses by the bidders would be reviewed for the following aspects of the proposed solution:

- What is the overall training plan and structure?
- One of the main training components will be user training. This will also include advanced training, in particular on (a) how to configure modules/ re-use and refine templates for the needs of individual field audit offices/ wings, (b) designing custom reports using the Reporting/ BI module. How does the training solution address this effectively?
- How will e-learning be used as part of the proposed training solution?
- Please give an illustrative extract of the training structure and content for a small component/ sub-component of training

Technical Presentation and Client Visit/ Client Interaction

The responses by the bidders (through the technical presentation and the client visit/ client interaction) would be reviewed for the following aspects:

Client Visit/ Client Interaction

- What were the risks that were foreseen in advance by the SI and handled proactively by the SI and client working together? Conversely, what were the risks that could have been, but were NOT foreseen in advance by the SI?
- What were the challenges that came up during project execution, and how were they handled by the SI and the client working together?
- Did the SI facilitate informed decision-making with regard to solution architecture etc. in terms of possible choices/ options and pros and cons thereof?
- What was the quality of staffing provided by the SI – key resources as well as the development team?
- Were there differences/ disagreements/ conflicts between the SI and client, how effective was the communication by the SI to facilitate early resolution?

Technical Presentation

- How well has the bidder (the key resources team making the technical presentation) understood our requirements? How do the key resources respond to our questions and requests for providing clarifications?
- What, in the opinion of the bidder, are the top technical and functional challenges (NOT logistical challenges) that are likely to be encountered in this Project? What are the kind of choices or suggestions or solutions that the bidder has in mind for IA&AD to consider?
- How does the bidder propose to implement Agile development methodology, given our requirements and timelines for Phase I, what are the Agile-specific challenges that could arise, and how could they be addressed?

7.7.4 IA&AD’s Right to ask for Revised Commercial Bid

After the Technical Evaluation and before opening of the Commercial Bid, IA&AD reserve the right to make changes to the specifications and Bill of Material. In this case, IA&AD shall ask for revised commercial Bids only for the revised scope from the Bidders that have been qualified in the technical evaluation.

7.7.5 Commercial Bid Evaluation

a. The Financial Bids of technically qualified Bidders will be opened on the prescribed date. Representatives from Technically qualified bidders may be present at the time of Financial Bid Opening.

b. If a bidder quotes NIL charges / consideration, the bid shall be treated as unresponsive and will not be considered.

c. Commercial Bids which are less than 65% of the average of the commercial bid values of the other technical qualified bidders will be disqualified. For calculating the average commercial bid value, the commercial bid values of all the bidders except of the bidder for which the bid is being evaluated shall be taken. This condition shall be applicable if at least three bidders qualify the Technical round.

Calculation for Commercial Bid of the Bidder = Sum total of (Value of Formats 3A + 3B+ 4A + 4B +4C + 4E + 5A + 5B + 5C + 6 +7 +8 + 50% x Format 4D) of Appendix II Financial Proposal Templates

d. **QCBS Evaluation**

The Bidder with the lowest qualifying financial bid (L1) will be awarded 100 score (amongst the Bidders which did not get disqualified on the basis of point c above). Financial Scores for other than L1 Bidders will be evaluated using the following formula:

Normalized Financial Score of a Bidder (Fn) = {(Commercial Bid of L1/Commercial Bid of the Bidder) X 100} (Adjusted to two decimal places)

e. Commercials for all components proposed by the bidder should be valid and firm for the period defined.

f. Labour rates, as shown in format 4D, 6 and 8 of Appendix II, as of 1st January 2020, shall be used while quoting the commercial bid. Escalation @ 8 % per annum, applicable on 1st January of every succeeding calendar year, will be applicable and paid for by IA&AD. Hence, labour costs should NOT be escalated in the commercial bid.

g. Cost quoted for the software (Tools, Software, system & application) must include all costs including the cost of procurement, customization/ configuration/ development and implementation, etc. as per RFP requirements and its maintenance for the entire project duration.

h. Cost quoted for the hardware must include the cost of procurement, supply at site, installation and configuration according to RFP requirements and its maintenance for the entire project duration.

i. The bidders are advised not to indicate any separate discount. Discount, if any, must be merged with the quoted prices. Discount of any type, indicated separately, shall not be taken into account for evaluation purpose for this RFP.

j. The bidders are required to distinctly mention the nature, percentage and amount of applicable taxes in appropriate columns.

k. Prices quoted in the bid must be firm and final and shall not be subject to any upward modifications.

l. A proposal submitted with an adjustable price quotation or conditional proposal may be rejected as non-responsive.

m. The bid price will include all taxes and levies and shall be in Indian Rupees.

n. IA&AD reserves the right to ask the bidder to submit proof of payment against any of the taxes, duties, levies indicated within specified time frames.

o. IA&AD reserves the right to ask the bidder to submit analysis of rate and data sheet for the rates quoted in the Commercial bid by the bidder

p. Prices must be quoted entirely in Indian Rupees.

q. All costs incurred due to delay of any sort, due to reasons attributable to the bidder, shall be borne by the bidder.

r. If the price for any of the services is not explicitly quoted in the commercial bid or mentioned as zero, it is assumed that the price for that particular element is absorbed in some other service element for which a price has been quoted, and IA&AD has the right to source services for which no price was quoted or quoted as zero, from the bidder at no additional price.

s. If taxes or any other applicable charges are not indicated explicitly, they are assumed to be bundled within the prices quoted and unbundling of these charges will not be entertained either during evaluation or while signing the agreement.

t. Bidders are advised to exercise adequate care in quoting the prices. No excuse for corrections in the quoted figures will be entertained after the proposals are submitted to IA&AD. All corrections, if any, should be initialled by the person signing the proposal form before submission, failing which the figures for such items may not be considered.

u. Any conditional bid would be rejected

v. Errors & Rectification: Arithmetical errors will be rectified on the following basis: “If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail”.

w. The amount stated in the Commercial proposal will be adjusted by IA&AD in accordance with the above procedure for the correction of errors and shall be considered as binding upon the bidder. If the bidder does not accept the corrected amount of the Commercial Proposal, its Proposal will be rejected.

x. No adjustment of the price quoted in the Commercial proposal shall be made on account of any variations in costs of labour (except as mentioned in para 7.7.5 f)) and materials, currency exchange fluctuations with international currency or any other cost component affecting the total cost in fulfilling the obligations under the agreement. No clauses for price fluctuations due to fluctuation of the Indian currency against any foreign currency will be accepted during the period of the agreement.

7.7.6 Combined and Final Evaluation

a. The technical and financial scores secured by each Bidder will be added using weightage of **<70%>** and **<30%>** respectively to compute a Composite Bid Score

b. The Bidder securing the highest Composite Bid Score will be adjudicated as the most responsive Bidder for award of the Project. The highest Composite Bid Score (Bn) will be calculated as follows:-

   <Bn = 0.70 * Tn + 0.30* Fn >

   Where

   Bn = overall score of Bidder

   Tn = Technical score of the Bidder (out of maximum of 100 marks)

   Fn = Normalized financial score of the Bidder (out of maximum of 100 marks)

c. In the event the highest composite bid score (Bn) (calculated to two decimal places) is 'tied' between two or more bidders, the Bidder securing the highest technical score will be adjudicated as the Best Value Bidder for award of the Project.

7.7.7 Notification of Award

Prior to the expiration of the validity period, IA&AD will notify the successful Bidder in writing or by email, that its proposal has been accepted (Letter of Intent - LOI). In case the tendering process / public procurement process has not been completed within the stipulated period, IA&AD may request the Bidders to extend the validity period of their Proposal.

The decision to extend the validity period of a Bidder's Proposal shall be the Bidder's sole prerogative.

7.8 Appointment of Systems Integrator

7.8.1 Award Criteria

IA&AD will award the Contract to the successful Bidder whose proposal has been determined to be substantially responsive and has been determined as the best value bid/ most responsive bid as per the process outlined above.

7.8.2 Right to Accept Any Proposal and To Reject Any or All Proposal(s)

IA&AD reserves the right to accept or reject any proposal, and to annul the tendering process/ Public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for IA&AD action.

7.8.3 IA&AD Contract finalization and award

IA&AD shall reserve the right to negotiate with the Bidder(s) whose Proposal has been ranked as the best value bid on the basis of Technical and Commercial Evaluation to the proposed Project, as per the guidance provided by Central Vigilance Commission (CVC).

7.8.4 Performance guarantee

A Performance Bank Guarantee (PBG) of 10% of total contract value of the contract would be furnished by the implementation agency in the form of a Bank Guarantee as per the format provided in the RFP from any **Commercial Bank**. The PBG should be furnished within **15 days** from notification of award or on or before signing of the contract, and should be valid till the entire term of the agreement and for an **additional period of 180 days** after the completion of term of agreement including warranty obligations.

In case any claims or any other contract obligations are outstanding, the Implementation Agency will extend the Performance Bank Guarantee as asked by the Purchaser till such time the Implementation Agency settles all claims and completes all contract obligations.

Notwithstanding what has been stated elsewhere in this Contract and the Schedules attached herein, in the event the Implementation Agency is unable to meet the obligations pursuant to the implementation of the Project and/or provide the operations and maintenance Services and any related scope of work as stated in this Contract, the Purchaser will, inter alia, have the option to invoke the Performance Bank Guarantee after serving a written notice fifteen days in advance on the Implementation Agency. Such right of the Implementation Agency shall be without prejudice to any other rights or remedies available under law or contract. In case the contract is extended, the PBG has to be valid for **180 days beyond the extended period**.

In the event of the expiry of this Agreement, IA&AD shall retain the Performance Bank Guarantee till it's validity period. Subsequently, the Performance Bank Guarantee shall be released provided IA&AD or an agency nominated by IA&AD certifies and IA&AD accepts that the handing over procedure as stated in the Exit Management Schedule has been duly complied with. In the event that the compliance is not completed, the Performance Bank Guarantee shall be invoked and the amount appropriated and forfeited. IA&AD will not pay any costs of Implementation Agency's conduct of business. There will be no payments to the Implementation Agency to compensate for business loss.

7.8.5 Signing of contract

Subsequent to receipt of valid Performance Guarantee from the successful Bidder, the parties shall enter into a contract, incorporating all clauses, pre-bid clarifications, the Proposal of the Bidder, terms and conditions regarding implementation of project, between IA&AD and the successful Bidder.

7.8.6 Downstream Work

IA&AD does not envisage any downstream work.

7.8.7 Repeat Order

IA&AD reserves the right to increase the quantity upto 25% as specified in the schedule of requirements without any change in the unit price or other terms and conditions within the agreed delivery schedule within a period of 3 years from the date of contract signing.

7.9 Integrity Pact

All the bidders shall submit the Integrity Pact agreement. Bidder shall upload scanned copies of the Integrity Pact agreement in Commercial Envelope on e-tendering system, without which the bid shall be rejected.

7.10 Failure to Agree with the Terms and Conditions of the RFP

Failure of the successful Bidder to agree with the Draft Legal Agreement and Terms & Conditions of the RFP may constitute sufficient grounds for the annulment of the award, in which event Purchaser may award the contract to the next best value Bidder or call for new proposals from the interested Bidders.

7.11 Fraud and Corrupt Practices

a. The Bidders/Bidders and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the Selection Process. Notwithstanding anything to the contrary contained in this RFP, IA&AD shall reject a Proposal without being liable in any manner whatsoever to the Bidder, if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice (collectively the “Prohibited Practices”) in the Selection Process. In such an event, IA&AD shall, without prejudice to its any other rights or remedies, forfeit and appropriate the Bid Security or Performance Security, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to the Authority for, inter alia, time, cost and effort of the Authority, in regard to the RFP, including consideration and evaluation of such Bidder’s Proposal.

b. Without prejudice to the rights of IA&AD under Clause above and the rights and remedies which IA&AD may have under the LOI or the Agreement, if any Bidder or Systems Implementation Agency, as the case may be, is found by the Authority to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the LOI or the execution of the Agreement, such Bidder or Systems Implementation Agency shall not be eligible to participate in any tender or RFP issued by the IA&AD during a period of three years from the date such Bidder or Systems Implementation Agency, as the case may be, is found by IA&AD to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.

c. For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them

   i. “corrupt practice” means:

      a) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the Selection Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of the IA&AD who is or has been associated in any manner, directly or indirectly with the Selection Process or the LOI or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of the IA&AD , shall be deemed to constitute influencing the actions of a person connected with the Selection Process);

or

b) save as provided herein, engaging in any manner whatsoever, whether during the Selection Process or after the issue of the LOI or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the LOI or the Agreement, who at any time has been or is a legal, financial or technical consultant/ adviser of IA&AD in relation to any matter concerning the Project;

ii. “fraudulent practice” means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process;

iii. “coercive practice” means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person’s participation or action in the Selection Process;

iv. “undesirable practice” means

a) establishing contact with any person connected with or employed or engaged by IA&AD with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or

b) having a Conflict of Interest; and

v. “restrictive practice” means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.

7.12 Conflict of Interest

a. A Bidder shall not have a conflict of interest that may affect the Selection Process or the Solution delivery (the **“Conflict of Interest”**). Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, the IA&AD shall forfeit and appropriate the EMD, if available, as mutually agreed genuine pre-estimated compensation and damages payable to IA&AD

for, inter alia, the time, cost and effort of the IA&AD including consideration of such Bidder's Proposal, without prejudice to any other right or remedy that may be available to the IA&AD hereunder or otherwise.

b. IA&AD requires that the System Integrator provides solutions which at all times hold the IA&AD 's interests paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work. The Implementation Agency shall not accept or engage in any assignment that would be in conflict with its prior or current obligations to other clients, or that may place it in a position of not being able to carry out the assignment in the best interests of the IA&AD .

c. Without limiting the generality of the above, a Bidder shall be deemed to have a Conflict of Interest affecting the Selection Process, if:

   i. the Bidder, its Associates (or any constituent thereof) and any other Bidder, its Associate (or any constituent thereof) have common controlling shareholders or other ownership interest; provided that this disqualification shall not apply in cases where the direct or indirect shareholding or ownership interest of an Bidder, its Associate (or any shareholder thereof having a shareholding of more than 5 per cent of the paid up and subscribed share capital of such Bidder or Associate, as the case may be) in the other Bidder or its Associate is less than 5% (five per cent) of the subscribed and paid up equity share capital thereof. For the purposes of this Clause, indirect shareholding held through one or more intermediate persons shall be computed as follows:

      - where any intermediary controlled by a person through management control or otherwise, the entire shareholding held by such controlled intermediary in any other person (the "Subject Person") shall be taken into account for computing the shareholding of such controlling person in the Subject Person; where a person does not exercise control over an intermediary, which has shareholding in the Subject Person, the computation of indirect shareholding of such person in the Subject Person shall be undertaken on

      - a proportionate basis; provided, however, that no such shareholding shall be reckoned under this Sub-clause if the shareholding of such person in the intermediary is less than 26% (twenty six per cent) of the subscribed and paid up equity shareholding of such intermediary; or

ii. a constituent of such Bidder is also a constituent of another Bidder; or

iii. such Bidder or its Associate receives or has received any direct or indirect subsidy or grant from any other Bidder or its Associate; or

iv. such Bidder has the same legal representative for purposes of this Application as any other Bidder; or

v. such Bidder has a relationship with another Bidder, directly or through common third parties, that puts them in a position to have access to each other's' information about, or to influence the Application of either or each of the other Bidder; or

there is a conflict among this and other Systems Implementation/Turnkey solution assignments of the Bidder (including its personnel and other members, if any) and any subsidiaries or entities controlled by such Bidder or having common controlling shareholders. The duties of the Systems Implementation Agency will depend on the circumstances of each case. While providing software implementation and related solutions to IA&AD for this particular assignment, the Systems Implementation Agency shall not take up any assignment that by its nature will result in conflict with the present assignment.

8 Deliverables & Timelines

The detailed schedule for the deliverables as given below can be mutually decided by discussion with selected vendor, before signing the contract. However, the timelines mentioned in Volume I, including Annexure A, of the RFP must be respected.

The table below depicts Track-wise deliverable along with corresponding timelines. The terms used here are based on Agile-Scrum, and can be suitably amended depending on the flavor of Agile proposed by the successful bidder.

Ref #	Deliverables for OIOS Solution	Details
Project Inception		
D1	Integrated Project Management Plan (IPMP) and Inception Report	▪ Project Kick-off ▪ Product Vision: Overarching goals of the project (intended end result of the project) ▪ DC/DR setting up plan ▪ Business Continuity Plan ▪ Warranty Service Plan ▪ Manpower Deployment Plan ▪ Key Project Roles (Product Owner, Development Team and Scrum Master) ▪ Communication plan ▪ Project Management plan (Timelines) ▪ Project Reporting Formats & Checklists
Track 1: Setting up of development and UAT environments		
D2	Product development plan	▪ DevOps Environment Sizing & Set-Up plan of Cloud Resources ▪ Agile Project Development Framework (Design, Development, user acceptance and testing plan)

D3	Cloud provisioning document (for development and UAT)	A report will be submitted upon completion of this activity and will include the following: ▪ Provisioning of Cloud Resource for initial development and UAT OIOS ▪ Deployment architecture mapping software and security components to IT Infrastructure deployed by SI ▪ Change & Release management ▪ Data Backup and Restore Plan ▪ Failover Testing Plan ▪ Management and Monitoring of IT Infrastructure components deployed.
D4	Migration plan (for migration of development and UAT, from cloud environment to DC/DR)	▪ Procedures and timelines to be followed for migration. ▪ Methodology to ensure completeness in migration. A report will be submitted upon completion of this activity and will include the following: ▪ System software, Hardware Resource for OIOS Implementation ▪ Deployment architecture mapping software and security components to IT Infrastructure deployed by SI ▪ Change & Release management ▪ Data Backup and Restore Plan ▪ Failover Testing Plan ▪ Management and Monitoring of IT Infrastructure components deployed
Track 2: OIOS Application design, development, roll out and implementation		
D5	Product backlog	▪ A prioritized list of all of the individual “user stories” for development in the overall project. ▪ Identify dependencies between user stories. ▪ Completion criteria for each user story. ▪ Ongoing revision and re-prioritization of the Product Backlog. ▪ Estimate of Effort required by the Development Team to develop each user story.

D6	Release planning document (for each release)	▪ Release backlog ▪ Minutes of release planning meeting
D7	Sprint planning document (for each sprint)	▪ Sprint backlog ▪ Sprint design document ▪ Minutes of sprint planning meeting ▪ Break down of user story into tasks. ▪ Assignment of task and timelines for completion.
D8	Sprint development document (for each sprint)	▪ Design, Code & test documentation ▪ Issue tracker for logging bugs – iteration wise ▪ Source code version tool repository ▪ Sprint metrics (Continuous monitoring) ▪ Sprint retrospective
D9	Sprint testing document (Stage 0)	▪ Test plans for user acceptance testing ▪ Results from user acceptance testing ▪ Issue tracker for logging UAT issues – iteration wise ▪ Sign-off from IA&AD on user acceptance testing
D10	Release testing document (Stage 1)	▪ Test plans for user acceptance testing (in most cases similar to Stage 0; However, test data would vary) ▪ Results from user acceptance testing ▪ Issue tracker for logging UAT issues – iteration wise ▪ Sign-off from IA&AD on user acceptance testing
D11	Release testing document (Stage 2)	▪ Test plans for user acceptance testing (in most cases similar to Stage 0 and Stage 1; However, test data would vary) ▪ Results from user acceptance testing ▪ Issue tracker for logging UAT issues – iteration wise ▪ Sign-off from IA&AD on user acceptance testing
D12	Release documentation	▪ Release notes ▪ User stories deferred for further releases ▪ Planned service disruption

		▪ Roll back strategy ▪ KPIs for successful roll-out
D13	Phase 1 testing document	▪ Test plans for Phase 1 acceptance testing (architectural consistency, integration of releases of phases 1 would also be additionally tested) ▪ Results from user acceptance testing ▪ Issue tracker for logging issues – iteration wise ▪ Sign-off from IA&AD on user acceptance testing
D14	Phase 2 testing document	▪ Test plans for Phase 2 acceptance testing (architectural consistency, integration of releases of phases 2 would also be additionally tested) ▪ Results from user acceptance testing ▪ Issue tracker for logging issues – iteration wise ▪ Sign-off from IA&AD on user acceptance testing
D15	Security Audit report (for each phase)	▪ Issue tracker for issues raised by STQC or CERT-In empanelled vendor – iteration wise ▪ Certificate of the auditor along with his report
D16	Data migration	▪ Data migration design documents ▪ Excel template for each data element or groups of data element which will be used by field audit offices for data migration ▪ Data migration guide for using Excel template
Track 3: Setting up of development, UAT, training, pre-production and production environment in PDC and DRC at Tier-3 co-located data centre		
D17	Hardware, System software provisioning document for production environment	A report will be submitted upon completion of this activity and will include the following: ▪ System software, Hardware Resource for OIOS Implementation ▪ Deployment architecture mapping software and security components to IT Infrastructure deployed by SI

		▪ Change & Release management ▪ Data Backup and Restore Plan ▪ Failover Testing Plan ▪ Management and Monitoring of IT Infrastructure components deployed
D18	Technology stack (licenses)	Installation, Configuration and Annual Technical Support of IA&AD owned licensed Technology Stack
Track 4: Centralized helpdesk set up and operations		
D19	Centralized Helpdesk Setup and Operations	▪ Helpdesk Resources; linked to Performance Issue Resolution Framework [for Development Team & End-Users]; ▪ Annual Technical Support of Helpdesk Software
Track 5: Training and capacity building		
D20	Training plan (for each training)	This document will cover the training plan and user manual, types of training, types of modules, frequency of training, location of training
D21	Training implementation document	▪ Schedule of training conducted ▪ Training Effectiveness ▪ Details of various participants in the workshops/trainings and their evaluations
D22	Training material	▪ Structure training modules ▪ Case studies
D23	User support	▪ Self-learning modules ▪ E-learning ▪ User manuals ▪ How-to training videos
Track 6: Operations and Maintenance		
D24	Contingency plan	▪ Emergency response procedures ▪ Backup arrangements, procedures, and responsibilities ▪ Disaster recovery procedures and responsibilities ▪ Business Continuity plan and procedures

D25	Resolution of Outstanding Issues Post Go-Live	▪ List of outstanding issues and corrective actions taken ▪ Corrective action taken by the SI and acceptance by IA&AD
D26	MIS reports	▪ IA&AD prefers to design the MIS reports and dashboards independently through the reporting/BI solution offered by the SI. However, SI shall design complex MIS reports and dashboards using the reporting/BI solution. The expected number of reports to be designed is a maximum of 500. Any request from IA&AD to design any report beyond 500 will be taken up as “Change management”
D27	Operations and maintenance	The periodic progress reports would summarize the following: ▪ Results of SLA accomplished during the prior period ▪ Cumulative deviations to date from schedule of progress milestones as specified in the agreed and finalized project plan ▪ Corrective actions to be taken to return to planned schedule of progress; proposed revisions to planned schedule ▪ Resources that the SI expects to be provided by the IA&AD and/or actions to be taken by the IA&AD in the next reporting period

9 Payment Schedules

The payment schedule including details of relevant conditions to be satisfied, payment mode, engagement model, frequency of billing and the principles involved in payment. The expected timeline for payment has been laid down by taking 'T' as the referential time frame, where T represents the date of signing of contract. It is important to note that these payment milestones are not the same as timelines for delivery of tracks. The non-delivery of the items in alignment with the timelines for delivery would trigger relevant penalty clauses mentioned in Vol 2 and Vol 3 of the RFP.

TRACK COST HEADS	PAYMENT CONDITION	PAYMENT OF	ENGAGEMENT MODEL & Frequency of billing	TIMELINES (T is the date of signing of the contract)	FORMAT	PRINCIPLES
TRACK 1: SETTING UP OF DEVELOPMENT & TEST ENVIRONMENT						
Approval of IPMP, Product backlog & resource deployment:	Approval of Integrated Project Management Plan Finalization of initial version of Product Backlog After Deployment of resources (onsite/offsite)	**5% of Development cost of OIOS Application Phase 1 & Phase 2***	Fixed Cost; One Time Cost (Lumpsum)	T+ completion of a, b and c	RFP volume 2, Appendix II Format 4A	
Setting Up of Development & other Environment	On successful commissioning of Dev & other environment with relevant software	**For Subscription Model components – On actuals**	For Subscription based – after 1st quarter For Perpetual based – 100%	T+ successful commissioning of Dev and other environments	Format 3A (Subscription) and 3B (Perpetual)	

TRACK COST HEADS	PAYMENT CONDITION	PAYMENT OF	ENGAGEMENT MODEL & Frequency of billing	TIMELINES (T is the date of signing of the contract)	FORMAT	PRINCIPLES
		after 1st quarter; For Perpetual license based components - 100% after one month of installation	after one month of installation			
TRACK 2: OIOS APPLICATION DEVELOPMENT, IMPLEMENTATION & ROLLOUT COST (PHASE-1)						
Stage 0 UAT	On completion of sprint demos as per prorated estimate of completed user stories as a proportion of estimated effort as per backlog Acceptance by Product Owner for functional part	**40%**	Fixed Cost; Every 2 Months invoice may be raised	Up to T + completion of phase 1 As per approved Estimate Backlog for Phase - 1 worked out by the SI in consultation with IA&AD	RFP volume 2, Appendix II Format 4A	Prorated estimate of completed user stories as a proportion of estimated effort as per Product backlog[1]
Stage 1 UAT (5 pilot offices)	On successful Stage 1 UAT in pilot offices	**20%**	Fixed Cost; (Every two months invoice may be raised)	Up to T + end of stage 1 implementation of phase 1	RFP volume 2, Appendix II Format 4A	As above

[1] For the purpose of payment , the pro-rate would be decided based on estimates in the initial sign off of product backlogs, notwithstanding any subsequent changes in the product back log

TRACK COST HEADS	PAYMENT CONDITION	PAYMENT OF	ENGAGEMENT MODEL & Frequency of billing	TIMELINES (T is the date of signing of the contract)	FORMAT	PRINCIPLES
Stage 2 UAT (nodal offices): Configurability for 26 nodal offices and HQ offices	On successful Stage 2 UAT in nodal offices	**20%**	Fixed Cost; (Every two months invoice may be raised)	Up to T + end of stage 2 implementation of phase 1	RFP volume 2, Appendix II Format 4A	As above
End of Phase – 1	At the end of Phase-1; On Integration Testing; all documentation and deliverables	**5%**	Fixed Cost; One time	At T + completion of phase 1	RFP volume 2, Appendix II Format 4A	On submission of final deliverables, documentation & integration testing
Post End of Quarter of Phase – 1 UAT	After one Quarter of M4	**10%**	Fixed Cost; One time	At T + one quarter after completion of phase 1	RFP volume 2, Appendix II Format 4A	As per Issue Register for Outstanding issues and Corrective action plan by SI
Phase-1 Procurement of System Software, hardware	On successful commissioning of System Software, hardware components of Phase - I	**80% on installation and 20% after commissioning at 5 sites**	Stage payments in 80:20	From 'T' to T + 6 Months	Format 4B (Perpetual)	
TRACK 2: OIOS APPLICATION DEVELOPMENT, IMPLEMENTATION & ROLLOUT COST (PHASE-2)						
Stage 0 UAT	On completion of sprint demos as per prorated estimate of completed user stories as a	**40%**	Fixed Cost; Every 2 Months	Up to T + up to completion of phase 2	RFP volume 2, Appendix II Format 4A	Prorated estimate of completed user stories as a proportion of

TRACK COST HEADS	PAYMENT CONDITION	PAYMENT OF	ENGAGEMENT MODEL & Frequency of billing	TIMELINES (T is the date of signing of the contract)	FORMAT	PRINCIPLES
	proportion of estimated effort as per backlog Acceptance by Product Owner for functional part			As per approved Estimate Backlog for Phase - 2 worked out by the SI in consultation with IA&AD		estimated effort as per Product backlog[2]
Stage 1 UAT (5 pilot offices)	On successful Stage 1 UAT in pilot offices	**20%**	Fixed Cost; Every 2 Months	Up to T + upto completion of stage 1 of phase 2 implementation.	RFP volume 2, Appendix II Format 4A	As above
Stage 2 UAT (nodal offices): Configurability for 26 nodal offices and HQ offices	On successful Stage 2 UAT in nodal offices	**20%**	Fixed Cost; Every 2 Months	Up to T + up to completion of stage 2 of phase 2 implementation	RFP volume 2, Appendix II Format 4A	As above
End of Phase – 2	At the end of Phase-2; On Integration Testing; all documentation and deliverables	**5%**	Fixed Cost;	At T + completion of phase 2	RFP volume 2, Appendix II Format 4A	On submission of final deliverables, documentation & integration testing
Post End of Quarter of Phase – 2 UAT	After One quarter of M4'	**10%**	Fixed Cost;	At	RFP volume 2, Appendix	As per Issue Register for Outstanding issues

[2] For the purpose of payment the pro rata would be decided based on review of product back log after completion of phase 1, this is not withstanding any subsequent changes in product backlog.

TRACK COST HEADS	PAYMENT CONDITION	PAYMENT OF	ENGAGEMENT MODEL & Frequency of billing	TIMELINES (T is the date of signing of the contract)	FORMAT	PRINCIPLES
				T+ One quarter after completion of phase 2	II Format 4A	and Corrective action plan by SI
Phase-2 Procurement of System Software	On successful commissioning of System Software, Hardware components of Phase - II	**80% on installation and 20% after OIOS Application commissioning at 5 offices**	Stage payments in 80:20	T + 12 Months	Format 4C	
TRACK 2: OIOS APPLICATION DEVELOPMENT, IMPLEMENTATION & ROLLOUT COST (PHASE-3)						
OIOS APPLICATION PHASE – 3	On fulfilment of work (as mutually agreed upon for the Resource, Time, work schedule before commencement of Phase-3 work)	**On Actuals**	Time and Material Every 2 Months	From T + completion of phase 2 to T + completion of phase 3	RFP volume 2, Appendix II, Format 4D	SI to raise an invoice every 2 months for Phase – 3 development basis the rate card in 3 bundles subject to mutual consultation
TRACK 3: SETTING UP OF PDC, DRC AND BACKUP SITES AT 2 IA&AD OFFICES						
PDC for OIOS Phase 1	On successful commissioning of System Software, Hardware components of Phase - II	**80% on installation and 20% after OIOS Application commissioning at 5 offices**	Stage payments in 80:20	T + completion of successful commissioning of all components for phase 1 to T + application commissioning in 5 offices	RFP volume 2, Appendix II Format 5A	

TRACK COST HEADS	PAYMENT CONDITION	PAYMENT OF	ENGAGEMENT MODEL & Frequency of billing	TIMELINES (T is the date of signing of the contract)	FORMAT	PRINCIPLES
PDC for OIOS Phase 2	On successful commissioning of System Software, Hardware components of Phase - II	**80% on installation and 20% after OIOS Application commissioning at 5 offices**	Stage payments in 80:20	T + completion of successful commissioning of all components for phase 2 to T + application commissioning in 5 offices	RFP volume 2, Appendix II Format 5B	
Setup DRC for OIOS	On Provisioning, configuration, testing & Set Up of DRC for OIOS	**80% on installation and 20% after OIOS Application commissioning at 5 offices**	Stage payments in 80:20	T + Completion of successful commissioning of all components of DRC to T + application commissioning at 5 offices	RFP volume 2, Appendix II Format 5C	
Storage Network Setup at 2 IA&AD offices	On Provisioning, configuration, testing & Set Up of Backup Site for OIOS at 2 IA&AD offices	**On actuals**	Fixed Cost; Quarterly	T to T + Completion of provisioning, configuration and successful testing of backup sites	RFP volume 2, Appendix II Format 5A, 5 C	
TRACK 4: CENTRALISED HELPDESK SETUP AND OPERATIONS						
Centralized Helpdesk Setup and Operations – All Activities	On Setup of: Centralised Helpdesk Software	**On actuals**	Time & Material for Resources; Quarterly	On Ongoing basis	RFP volume 2, Appendix II Format 6	SI to raise an invoice for actuals on setup of centralised helpdesk and deployment of

TRACK COST HEADS	PAYMENT CONDITION	PAYMENT OF	ENGAGEMENT MODEL & Frequency of billing	TIMELINES (T is the date of signing of the contract)	FORMAT	PRINCIPLES
	Deployment of Helpdesk Resources Operationalisation of Issue Resolution Framework for Development Team and End-user					helpdesk resources and operationalisation of Issue Resolution Framework
TRACK 5: TRAINING & CAPACITY BUILDING						
Training of Product Owner's Core Team	On completion of training batches for training on Agile Software Engineering Training	**On actuals**	For each Training conducted Quarterly	T to T + completion of delivery of all training requirements	RFP volume 2, Appendix II Format 7	SI to raise an invoice every quarter for actuals on completion of training batches, delivery of e-training support
Master Training OIOS Phase 1 & 2	On completion of training batches for Master training on OIOS Phase 1 & 2	**On actuals**	For each Training conducted Quarterly	T to T + completion of delivery of all training requirements	RFP volume 2, Appendix II Format 7	SI to raise an invoice every quarter for actuals on completion of training batches, delivery of e-training support
UAT training Phase 1 and 2	On completion of training batches for UAT training	**On actuals**	For each Training conducted Quarterly	T to T + completion of delivery of all training requirements	RFP volume 2, Appendix II Format 7	SI to raise an invoice every quarter for actuals on completion of training batches, delivery of e-training support
TRACK 6: OPERATIONS AND MAINTENANCE						

TRACK COST HEADS	PAYMENT CONDITION	PAYMENT OF	ENGAGEMENT MODEL & Frequency of billing	TIMELINES (T is the date of signing of the contract)	FORMAT	PRINCIPLES
OIOS Phase 1 and Phase 2	On successfully meeting the SLAs	**EQIs**	Fixed Cost Quarterly	From date of go live of Phase 2 UAT, for 7 years	RFP volume 2, Appendix II Format 8	SI to raise an invoice every quarter for O&M payments subject to meeting the Service Level Agreement (SLAs)

Appendix I. Pre-Qualification & Technical Bid Templates

The Bidders are expected to respond to the RFP using the forms given in this section and all documents supporting Pre-Qualification / Technical Evaluation Criteria.

Pre-Qualification Bid & Technical Proposal shall comprise of following forms:

Forms to be used in Pre-Qualification Proposal

- Format 1: Compliance Sheet for Pre-qualification Proposal
- Format 2: Particulars of the Bidder
- Format 3: Bank Guarantee for Earnest Money Deposit

Forms to be used in Technical Proposal

- Format 4: Compliance Sheet for Technical Proposal
- Format 5: Letter of Proposal
- Format 5A: Project Citation Format
- Format 6: Track 1: Setting Up of Development & Test Environment
- Format 7: Effort Estimate for Development of OIOS Phase 1 Application
- Format 7A: Team composition with quantity.
- Format 7B: Resource Deployment Plan for OIOS Application Phase 1
- Format 8: Key Personnel
- Format 8A: Curriculum Vitae (CV) of Key Personnel
- Format 9: Solution Proposed
- Format 9A: Software Architecture and Design to meet the Non Functional Requirements
- Format 9B: Sizing of Compute resources w.r.t to OIOS Phase 1 requirements and comply to SLAs
- Format 10: Software Engineering Approach: OIOS Application
- Format 10A: Software Engineering Approach: OIOS Application Phase 1, 2
- Format 10B: Software Engineering Approach: OIOS Application Phase 3
- Format 11: Project Delivery and Management Plan
- Format 12: Training Plan
- Format 13: Operations and Maintenance Plan
- Format 14: Exit Management Plan

- Format 15 : Proposed BoM Matrix of the components for the Track 2: Middleware and Software requirements
- Format 15 A. Phase 1: Middleware and System Software
- Format 15 B. Phase 2: Middleware and Software specifications
- Format 16: Specifications Card Matrix of the components for Track 3: Phase 1
- Format 16 A. Phase 1 at PDC: Hardware
- Format 16 B. Security at PDC
- Format 16 C. Setting up of Backup Site 1 and Lease Line Provisioning
- Format 17: Requirement of the components for Track 3: Phase 2
- Format 17 A. Phase 2: Middleware and Software
- Format 18: Requirements of the components for Track 3: DRC
- Format 18 A. Disaster Recovery Center: Hardware
- Format 18 B. Disaster Recovery Center: System Software
- Format 18 C. Setting up of Backup Site 2 and Lease Line Provisioning
- Format 19: Proposed Work Plan
- Format 20: Illustrative Manufacturers'/Producers’ Authorization Form
- Format 21: Client References

Format 1. Compliance Sheet for Pre-qualification Proposal

The pre-qualification proposal should comprise of the following basic requirements. The documents mentioned in this compliance sheet along with this form, needs to be a part of the Pre-Qualification proposal

S No	Basic Requirement	Documents Required	Provided	Reference & Page Number
1.	Letter of Proposal	As per (Appendix I - Format 5)	Yes / No	
2.	Power of Attorney	Copy of Power of Attorney in the name of the Authorized signatory	Yes / No	
3.	Particulars of the Bidders	As per (Appendix I - Format 2)	Yes / No	
4.	EMD	Demand Draft / Bank Guarantee (Appendix I - Format 3)	Yes / No	
5.	Legal Entity	Certificate of incorporation Registration Certificates	Yes / No	
6.	Statutory Tax Registrations	Copy of PAN Card Copy of GST Registration Certificate	Yes / No	
7.	Sales turnover from IT Consultancy/ IT Advisory Services	Extracts from the audited balance sheet and profit & loss for the last 3 years OR Certificate from the statutory auditor or Chartered Accountant for the last 3 years	Yes / No	
8.	Net worth Requirements	Auditor's / Company Secretary or Chartered Accountant Certificate mentioning Net-Worth	Yes / No	
9.	Certifications	Copy of Certificates (i) Valid CMMI Level 5 (ii) ISO 27001	Yes / No	
10.	Blacklisting and Debarment	A Self Certified letter that the bidder (or any of its successor) is not in the	Yes / No	

S No	Basic Requirement	Documents Required	Provided	Reference & Page Number
		active debarred list - published by GeM or Central Procurement Portal or Procuring Ministry/Dept/Agency /IA&AD		
11.	Technical Capacity	Copy of work order / client certificates. OR Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor);	Yes / No	
12.	Experience in Data Center	Copy of work order / client certificates. Completion certificates from the client; OR Work order + Self certificate of completion with details	Yes / No	
13.	Manpower Strength	Self-Certification by the authorized signatory with clear declaration of staff – year wise, level/designation wise.	Yes / No	

Format 2. Particulars of the Bidder

S No	Information Sought	Details to be Furnished
A.	Name and address of the bidding Company	
B.	Incorporation status of the firm (public limited / private limited, etc.)	
C.	Year of Establishment	
D.	Date of registration	
E.	ROC Reference No.	
F.	Details of company registration	
G.	Details of registration with appropriate authorities for service tax	
H.	Name, Address, email, Phone nos. and Mobile Number of Contact Person	

Format 3. Bank Guarantee for Earnest Money Deposit

To,

<Name>

<Designation

<Address>

<Phone Nos.>

<email id>

Whereas <<Name of the Bidder>> (hereinafter called 'the Bidder') has submitted the bid for Submission of RFP # <<RFP Number>> dated <<Date>> for <<Implementation of One IAAD and One System>> (hereinafter called "the Bid") to IA&AD

Know all Men by these presents that we << >> having our office at <<Address>> (hereinafter called "the Bank") are bound unto the Comptroller and Auditor General of India, (hereinafter called "the Purchaser") in the sum of Rs. <<Amount in figures>> (Rupees <<Amount in words>> only) for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this <<Date>>

The conditions of this obligation are listed in Section 7.3.3 of Vol II of the RFP:

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or more of the conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to <<insert date>> and including <<extra time over and above mandated in the RFP>> from the last date of submission and any demand in respect thereof should reach the Bank not later than the above date.

NOTHWITHSTANDING ANYTHING CONTAINED HEREIN:

I. Our liability under this Bank Guarantee shall not exceed Rs. <<Amount in figures>> (Rupees <<Amount in words>> only)

II. This Bank Guarantee shall be valid upto <<insert date>>)

III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before <<insert date>>) failing which our liability under the guarantee will automatically cease.

IV. We also undertake not to revoke this guarantee during this period except with the previous consent of the Purchaser in writing and we further agree that our liability under the EMD / Bid Security shall not be discharged by any variation in the term of the said RFP and we shall be deemed to have agreed to any such variation.

V. No interest shall be payable by the Purchaser to the bidder on the guarantee for the period of its currency.

(Authorized Signatory of the Bank) Seal:

Date:

Format 4. Compliance Sheet for Technical Proposal

S No	Basic Requirement	Documents Required	Provided	Reference & Page Number
1.	Letter of Proposal	As per Appendix I, Format 5		
2.	Technical Proposal covering: ▪ Proposal on OIOS Application Functionality ▪ Technologies proposed for OIOS Application ▪ Project Methodology, Support and Documentation ▪ Training Plan ▪ Profile of proposed team members ▪ Exit Management	Technical Proposal as per the Formats (Format 4 to 21) specified in Appendix I.		
3.	Compliance to the functional requirements stated in RFP Vol1 Annexure A	Functional Requirement Compliance Sheet		

Format 5. Letter of Proposal

To:

<Location, Date>

<Name>

<Designation>

<Address>

<Phone Nos.>

<email id>

Subject: Submission of the Technical bid for Implementation of One IA&AD One System assignment

Dear Sir/Madam,

We, the undersigned, offer to provide Systems Integration solutions to IA&AD on Implementation of One IA&AD One System with your Request for Proposal dated <insert date> and our Proposal. We are hereby submitting our Proposal, which includes this Technical bid and the Financial Bid sealed on the https://eprocure.gov.in/eprocure/app portal

We hereby declare that all the information and statements made in this Technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification.

We undertake, if our Proposal is accepted, to initiate the System Integration services related to the assignment within 15 days of signing of the contract. We agree to abide by all the terms and conditions of the RFP document. We would hold the terms of our bid valid for 180 days as stipulated in the RFP document.

We understand you are not bound to accept any Proposal you receive.

Yours sincerely,

Authorized Signature [In full and initials]: ---

Name and Title of Signatory: ---

Name of Firm: --

Address:--

Location:---Date:---

Form 5A. Project Citation Format

Relevant IT project experience (provide no more than 5 projects in the last 5 years)	
General Information	
Name of the project	
Client for which the project was executed	
Name and contact details of the client	
Project Details	
Description of the project	
Scope of services	
Service levels being offered/ Quality of service (QOS)	
Technologies used	
Outcomes of the project	
Other Details	
Total cost of the project	
Total cost of the services provided by the respondent	
Duration of the project (no. of months, start date, completion date, current status)	
Other Relevant Information	
Letter from the client to indicate the successful completion of the projects	
Copy of Work Order	

Format 6. Track 1: Setting Up of Development & Test Environment

Service Provider			**<<Name of Proposed CSP>>**	
Cloud Resource Service Period in months*			**03**	
S No	**Item**	**Unit of Measurement**	**Quantity**	**Number of Months**
1.	**VM (loaded with latest Linux or Windows environment which bidder selects for development)**			
1.1	X86 16Core with 64 GB RAM	Number	1	03

S No	Item	Unit of Measurement	Quantity	Number of Months	OEM, Make & Model
2.	**Storage**				
2.1.	SSD 500 GB	Number	1	03	
2.2.	SAS / NLSAS 500 GB	Number	1	03	

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
3.	**System Software**			
3.1.	Software development Licenses for Dev Team	License	As required	
3.2.	Application Server	License	As required	
3.3.	Database Server	License	As required	
3.4.	BPM	License	As required	
3.5.	GIS	License	As required	
3.6.	Any other	License	As required	

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
4.	**Supporting Platform**			

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
4.1.	Help desk Tool – OIOS	License	1	
4.2.	Web conferencing tool (Helpdesk - multiple offices)	Host	10	
4.3.	KMS Platform, discussion forum & Implementation	License	1	
4.4.	Document management system	Core	4	

Note: Sl No 4 - Perpetual license/ support (COTS/ Open source software)

Format 7. Effort Estimate for Development of OIOS Phase 1 Application

<< To be filled by SI>>

Format 7A. Team composition with quantity

<<To be filled by SI>>

Format 7B. Resource Deployment Plan for OIOS Application Phase 1

No	Name of Staff	Staff input in Months (in the form of a bar chart)2													Total staff man months proposed
		1	2	3	4	5	6	7	8	9	10	11	12	n	Total
1															
2															
3															
4															
n															
												Total			

1. Professional Staff the input should be indicated individually; for Support Staff it should be indicated by category
2. Months are counted from the start of the assignment.

▬ Full time input ▭ Part time input

Format 8. Key Personnel

<< To be filled by SI>>

Format 8A. Curriculum Vitae (CV) of Key Personnel

General Information	
Name of the person	
Current Designation / Job Title	
Current job responsibilities	
Proposed Role in the Project	
Proposed Responsibilities in the Project	
Academic Qualifications: • Degree • Academic institution graduated from • Year of graduation • Specialization (if any) • Key achievements and other relevant information (if any)	
Professional Certifications (if any)	
Total number of years of experience	
Number of years with the current company	
Summary of the Professional / Domain Experience	
Number of complete life cycle implementations carried out	
Past assignment details (For each assignment provide details regarding name of organizations worked for, designation, responsibilities, tenure) Prior Professional Experience covering: • Organizations worked for in the past • Organization name	

• Duration and dates of entry and exit • Designation Location(s) • Key responsibilities • Prior project experience • Project name • Client • Key project features in brief • Location of the project • Designation • Role • Responsibilities and activities • Duration of the project Please provide only relevant projects.	
Proficient in languages (Against each language listed indicate if peak/read/write)	

Format 9. Solution Proposed

Technical approach, methodology and work plan are key components of the Technical Proposal. You are suggested to present Approach and Methodology as follows:

a) Requirements specified in RFP Vol-I, Annexure A, B and C
b) Requirements specified in Technical evaluation criteria of RFP Vol-2
c) Any other requirement felt necessary

Format 9 A. Software Architecture and Design to meet the Non Functional Requirements

Requirements specified in RFP Vol-I, Annexure B.

Format 9 B. Sizing of resources w.r.t to OIOS Phase 1 requirements and comply to SLAs

Requirements specified in RFP Vol-I, Annexure C.

Format 10. Software Engineering Approach: OIOS Application

Software Engineering Approach to develop and implement OIOS Phase 1 requirements using Agile methodology.

Format 10 A. Software Engineering Approach: OIOS Application Phase 1, 2

Software Engineering Approach to develop and implement OIOS Phase 1, 2 requirements.

Format 10 B. Software Engineering Approach: OIOS Application Phase 3

Software Engineering Approach to develop and implement OIOS Phase 3 requirements.

Format 11. Project Delivery and Management Plan

Project Delivery and Management Plan covering all the project tracks for successfully delivering OIOS project is to be submitted by SI.

Format 12. Training Plan

<< To be filled by SI>>

Format 13. Operations and Maintenance Plan

<< To be filled by SI>>

Format 14. Exit Management Plan

<<To be filled by SI>>

Format 15 Proposed BoM Matrix of the components for the Track 2: Middleware and Software requirements

Format 15 A. Phase 1: Middleware and System Software

S No	Production Environment	Unit of Measurement	Quantity	OEM, Make & Model
	Supporting Platform			
1.	Operating system – Open source	Support	As required	
2.	Operating system - COTS	License/	As required	
3.	Virtualisation software	License/ CPU	As required	
4.	Virtualisation Manager Software	License/ Support	1	
5.	**Core System Software Components**			
5.1.	Web server	Core	4	
5.2.	Application Server	Core	4	
5.3.	BPM Software	Core	4	
5.4.	Document management system	Core	4	
5.5.	Database – OIOS	Core	4	
5.6.	Database security - OIOS	Core	4	
5.7.	KMS Platform, discussion forum & Implementation	License	1	
5.8.	Help desk Tool – OIOS	License	1	
5.9.	Web conferencing tool (Helpdesk - multiple offices)	Host	10	
6.	SIEM	License	As required	
7.	Identity access and management (for 29,000 users) – 25% Delivery	License		
8.	**EMS Software**			

S No	Production Environment	Unit of Measurement	Quantity	OEM, Make & Model
8.1.	Monitoring: IT Infrastructure (device based - OS Instances: Server OS, Virtualisation, Firewall, IPS, Storage)	Number	As required	
8.2.	Monitoring: OIOS Application Performance (Real User Monitoring, Diagnostics)	License	As required	
8.3.	Dashboard & Reporting (Events co-relation, Centralized Reporting)	License	As required	
8.4.	Service Desk (SLA monitoring, Incident Mgmt.)	License	As required	
8.5.	OIOS, IT Infrastructure Operational Analytics (Log Correlation & Analysis)	License	As required	

Notes:

1. **Sl no 1-3**: SI need to fill quantity as per proposed solution and delivery shall be limited to number of VMs planned for this Phase only
2. **Core System Software Components (Sl no 5.1-5.6):** The system software components specified here need to be provisioned as per estimated usage. For Phase-2, same components shall be provisioned as per details provided later in Phase-2 section.

Timelines: 03 Months from Date of Agreement signing.

Format 15 B. Phase 2: Middleware and Software specifications

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
1.	**RDBMS Instance**			
1.1.	MySQL	Core	4	
1.2.	PostgreSQL	Core	4	
1.3.	MS SQL server	Core	4	
1.4.	DB2	Core	4	
1.5.	Oracle	Core	4	

Note: Latest version of standard edition..

Format 16 Specifications Card Matrix of the components for Track 3: Phase 1

Format 16 A. Phase 1 at PDC: Hardware

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
1.	Blade server chassis	Number	1	
2.	Blade Servers with 2X16 cores (Total 96 Cores)	Number	3	
3.	KVM Switch	Number	2	
4.	SAN storage 40 TB Usable	License/ Support	1	
5.	Racks	Number	As required	
6.	SAN Switch 24 Port	Number	2	
7.	Access switch 10G	Number	4	
8.	Structured Cabling within DC (Cat 6 A	Job	1	

Timelines: 03 Months from Date of Agreement signing.

Note:

1. DMZ, MZ segregation shall be done using Firewall.
2. A separate management zone shall be created for deployment of Management and Monitoring Solution/ tools, using Access switch

Format 16 B. Security at PDC

S No	Item	Unit of Measure ment	Quantity	OEM, Make & Model
1.	**Security**			
1.1	Firewall Next Generation with SSL VPN (2 GBPS cumulative throughput including IPS, etc.)	Number	2	
1.2	IPS	No	2	
1.3	Application Security	Subscription/ Year	2	
1.4	URL filtering	Subscription/ Year	2	
1.5	Anti-APT Solution with sand-boxing	Subscription/ Year	1	
1.6	Web application firewall	No	2	
1.7	DLP (System administrators console)	License	As required	
1.8	HIPS	License	As required	
1.9	Privilege Management of System Administrator (VMs, Physical Servers, Storage)	LIC / VM	As required	
1.10	Database Activity Monitoring	License	As required	
1.11	HSM	Number	1	
1.12	Anti-Virus –malware and Anti-Spam (for Server & System administration OS)	Subscription/ Year	As required	

Format 16 C. Setting up of Backup Site 1 and Lease Line Provisioning

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
1.	**Backup Site/NLDC**			
1.1	SAN (SAS based, 10TB usable capacity, expendable to 20TB usable)	Number	1	
1.2	UPS (To support above SAN, with 30 min power backup)	Number	1	
2.	**Lease line provisioning**			
2.1	PDC to Backup Site 1/NLDC	Number	1	
2.2	PDC to NICNET Gateway 1	Number	1	

Format 17. Requirement of the components for Track 3: Phase 2

Format 17 A. Phase 2: Middleware and Software

S No	Production Environment	Unit of Measurement	Quantity	OEM, Make & Model
1.	**Blade Servers with 2X16 cores**	Number	7	
2.	**Supporting Platform**			
2.1	Operating system – Open source	Support	As required	
2.2	Operating system - COTS	License/	As required	
2.3	Virtualisation software	License/ CPU	As required	
3.	**Core System Software Components**			
3.1	Web server	Core	4	
3.2	Application Server	Core	4	

S No	Production Environment	Unit of Measurement	Quantity	OEM, Make & Model
3.3	BPM Software	Core	4	
3.4	Document management system	Core	4	
3.5	Database – OIOS	Core	12	
3.6	Database security - OIOS	Core	12	
3.7	Database Administration Software Tool for DBA	User License	10	
3.8	GIS Server with map updation	Core	8	
3.9	Identity access and management (for 29,000 users) – 75% Delivery			

Format 18. Requirements of the components for Track 3: DRC

Format 18 A. Disaster Recovery Center: Hardware

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
1.	Blade server chassis	Number	1	
2.	Blade Servers with 2X16 cores (Total 128 Cores) *	Number	4	
3.	KVM Switch	Number	2	
4.	SAN storage 40 TB Usable	License/ Support	1	
5.	Racks	Number	As required	
6.	SAN Switch 24 Port	Number	2	
7.	Access switch 10G	Number	4	
8.	Structured Cabling within DC (Cat 6 A)	Job	1	

* 128 X86 Cores

Format 18 B. Disaster Recovery Center: System Software

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
1.	**Security**			
1.1.	Firewall Next Generation with SSL VPN (1 GBPS cumulative throughput including 7.2, 7.3 and 7.4)	Number	2	
1.2.	IPS	No	2	
1.3.	Application Security	Subscription/Year	2	
1.4.	URL filtering	Subscription/Year	2	

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
1.5.	Anti-APT Solution with sand-boxing	Subscription/Year	1	
1.6.	Web application firewall	No	2	
1.7.	DLP (System administrators console)	License	As required	
1.8.	HIPS	License	As required	
1.9.	Privilege Management of System Administrator (VMs, Physical Servers, Storage)	LIC / VM	As required	
1.10.	Database Activity Monitoring	License	As required	
1.11.	HSM	Number	1	
1.12.	Anti-Virus –malware and Anti-Spam (for Server & System administration OS)	Subscription/Year	As required	

S No	Item	Unit of Measurement	Quantity	OEM Make & Model
1.	**Software**			
1.1	Site Recovery Software	License/DR	1	
1.2	Web server	Core		
1.3	Application Server	Core		
1.4	BPM Software	Core		
1.5	Document management system	Core		
1.6	Database – OIOS	Core		
1.7	Database security - OIOS	Core		
1.8	Identity access and management	License		
1.9	GIS Server	Core		

Note: The above list is for illustration purpose only. The SI must decide the Software components (50% of PDC) which need additional licenses for PDC/DRC operations as per defined RPO, RTO and SLAs.

Format 18 C. Setting up of Backup Site 2 and Lease Line Provisioning

S No	Item	Unit of Measurement	Quantity	OEM, Make & Model
1.	**Backup Site/NLDC**			
1.1	SAN (SAS based, 10TB usable capacity, expendable to 20TB usable)	Number	2	
1.2	UPS (To support above SAN, with 30 min power backup)	Number	2	
2.	**Lease line provisioning**			
2.1	Leased line between PDC, DCR of 50 Mbps	Number	1	
2.2	PDC to Backup Site 2/NLDC	Number	2	
2.3	DCR to NICNET Gateway 2	Number	1	

Format 19. Proposed Work Plan

No	Activity[1]	Calendar Months												
		1	2	3	4	5	6	7	8	9	10	11	12	n
1														
2														
3														
4														
5														
N														

I. Indicate all main activities of the assignment, including delivery of reports (e.g.: inception, interim, and final reports), and other benchmarks such as Purchaser approvals. For phased assignments indicate activities, delivery of reports, and benchmarks separately for each phase.

II. This should be suitably adapted to the Agile-based software development methodology proposed by the bidder.

Format 20. Illustrative Manufacturers'/Producers' Authorization Form

[This form has to be provided by the OEMs of the products proposed]

No. Date:

To:

OEM Authorization Letter

Dear Sir,

Ref: Your RFP Ref: [*] dated [*]

We who are established and reputable manufacturers / producers of having factories / development facilities at (address of factory / facility) do hereby authorize M/s

(Name and address of Agent) to submit a Bid, and sign the contract with you against the above Bid Invitation.

We hereby extend our full guarantee and warranty for the Solution, Products and services offered by the above firm against this Bid Invitation.

We also undertake to provide any or all of the following materials, notifications, and information pertaining to the Products manufactured or distributed by the Supplier:

a. Such Products as IA&AD opt to purchase from the Supplier, provided, that this option shall not relieve the Supplier of any warranty obligations under the Contract; and

b. in the event of termination of production of such Products:

    i. advance notification to IA&AD of the pending termination, in sufficient time to permit the Bank to procure needed requirements; and

    ii. Following such termination, furnishing at no cost to IA&AD , the blueprints, design documents, operations manuals, standards, source codes and specifications of the Products, if requested.

We duly authorize the said firm to act on our behalf in fulfilling all installations, Technical support and maintenance obligations required by the contract.

Yours faithfully,

(Name)

(Name of Producers)

Note: This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer. The Bidder in its Bid should include it.

Format 21. Client References

Please indicate details of three client references, who would be willing to interact (either face to face or through a video/ teleconference) with the IA&AD Evaluation Team and/or permit a client visit by the IA&AD Evaluation Team. The issues to be covered in the client visit/ client interaction are mentioned in the Technical Evaluation Model. The client references should involve a development project, and not be restricted to infrastructure provision.

Interaction with the client will be kept confidential by the IA&AD Evaluation Team and will not be used for any purpose than the technical evaluation for this RFP.

Name of Client Institution:

Client Project Manager:

Phone:

E-mail:

Scope of SI Project:

Period during which SI Project executed:

Appendix II. Financial Proposal Templates

Format 1. Covering Letter

To: <Location, Date>

<Name>

<Designation>

<Address>

<Phone Nos.>

<email id>

Subject: Submission of the Financial bid for Implementation of One IAAD One System

Dear Sir/Madam,

We, the undersigned, offer to provide the Implementation services for Implementation of One IAAD One System in accordance with your Request for Proposal dated <<Date>> and our Proposal (Technical and Financial Proposals). Our attached Financial Proposal is for the sum of <<Amount in words and figures>> (Value **A** of Format 2 of Appendix II). This amount is inclusive of taxes.

1. PRICE AND VALIDITY

- All the prices mentioned in our Tender are in accordance with the terms as specified in the RFP documents. All the prices and other terms and conditions of this Bid are valid for a period of **<days>** calendar days from the date of bid submission closing.
- We hereby confirm that our prices include all taxes. However, all the taxes are quoted separately under relevant sections.
- We understand that the actual payment would be made as per the existing indirect tax rates during the time of payment.

2. UNIT RATES

We have indicated in the relevant forms enclosed, the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

3. TENDER PRICING

We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in Tender documents.

4. QUALIFYING DATA

We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our Tender, we agree to furnish the same in time to your satisfaction.

5. BID PRICE

We declare that our Bid Price is for the entire scope of the work as specified in the <Refer Section No.>. These prices are indicated in the Commercial Bid attached with our Tender as part of the Tender.

6. PERFORMANCE BANK GUARANTEE

We hereby declare that in case the contract is awarded .to us, we shall submit the Performance Bank Guarantee as specified in the <Appendix III> of this RFP document.

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal, i.e., [Date].

We understand you are not bound to accept any Proposal you receive.

We hereby declare that our Tender is made in good faith, without collusion or fraud and the information contained in the Tender is true and correct to the best of our knowledge and belief.

We understand that our Tender is binding on us and that you are not bound to accept a Tender you receive.

Thanking you,
We remain,

Yours sincerely,

Authorized Signature:

Name and Title of Signatory:

Name of Firm:

Address:

Format 2. TOTAL COMMERCIAL QUOTE

S .No	Form Reference	Track Name	Format Number	Project Component Name	Project Component Cost (INR)	Track Cost (INR)
1.	Format 3	**Track 1:** Setting Up of Development & Test Environment	Format 3A	Track 1 - Cloud Resource Cost Format		
			Format 3B	Track 1: System Software Cost		
2.	Format 4	**Track 2:** OIOS Application Design, Development, Implementation and Rollout	Format 4A	OIOS Application Design, Development, Implementation and Rollout		
			Format 4B	Track 2: Phase 1 Middleware and Software		
			Format 4C	Track 2: Phase 2 Middleware and Software		
			Format 4D	Phase 3 Development Team		
			Format 4E	OIOS Application Cloud to PDC Migration Cost		
3.	Format 5	**Track 3:** Setting Up of PDC and DRC and Backup Sites at 2 IA&AD offices	Format 5A	Track 3: Phase 1 - Setting Up of PDC		
			Format 5B	Track 3: Phase 2 - Setting Up of PDC		
			Format 5C	Track 3: Phase 2 - Setting Up of DRC		
4.	Format 6	**Track 4:** Centralized Helpdesk Set Up and Operations				
5.	Format 7	**Track 5:** Training Cost				
6.	Format 8	**Track 6:** Operations and Maintenance Cost				
A.	**Total Cost (1+2+3+4+5+6) in Numbers**					
	Total Cost in Words:					

Format 3. Track 1: Setting Up of Development & Test Environment

FORMAT 3A		Track 1 - Cloud Resource Cost Format						
#	**Item**	**Unit of Measurement**	**Quantity**	**Number of Months**	**Price Per Unit Per Month**	**Total Price (excluding taxes)**	**Tax in %age**	**Total Price (including taxes)**
			A	**B**	**C**	**D = A x B x C**	**E**	**F =D + (D x E/100)**
All Amount to be quoted in INR								
1.	**VM (loaded with latest Linux or Windows environment which the bidder selects for development)**							
1.1.	X86 64Core with 256GB RAM*	Number	1	3				
Row Intentionally left Blank								
2.	**Storage**							
2.1.	SSD 500 GB	Number	1	3				
2.2.	SAS / NLSAS 500 GB	Number	1	3				
Row Intentionally left Blank								
	Total Cost (In Numbers) Including Taxes							
	Total Cost (In Words) Including Taxes							

* Cumulative size of 3 VMs will be 64 Core and 256 GB RAM respectively

FORMAT 3B			Track 1: System Software Cost													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
All Amount to be quoted in INR																
1.1.	**Software development licenses for dev team**		License	As required												
1.2.	Application Server		License	As required												
1.3.	Database Server		License	As required												
1.4.	BPM		License	As required												
1.5.	GIS		License	As required												

FORMAT 3B			Track 1: System Software Cost													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
1.6.	Any other		License	As required												
	Total Cost (In Numbers) Including Taxes															
	Total Cost (In Words) Including Taxes															

Note: In case of Open Source Software, Unit Rate (B) may be zero.

Format 4. Track 2: OIOS Application Design, Development, Implementation and Rollout

FORMAT 4A	OIOS Application Design, Development, Implementation and Rollout				
S No	**Components Name**	**Unit**	**Total Capex (Excluding Taxes)**	**Taxes %**	**Total Capex (Inclusive of Taxes)**
			A	**B**	**C = A + (A*B/100)**
All Amount to be quoted in INR					
A	**OIOS Phase 1 - Bespoke Software Development**	Lumpsum			
B	**OIOS Phase 2 - Bespoke Software Development**	Lumpsum			
Row Intentionally left Blank					
C	***Total Cost (In Numbers) Including Taxes***				
	Total Cost (In Words) Including Taxes				

Note: OIOS Phase 2 should be quoted on the basis of offsite deployment in this table. Onsite premium, if any, for onsite deployment of the entire development team in IA&AD premises, should be quoted in percentage terms.

FORMAT 4B			Track 2: Phase 1 Middleware and Software													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
			Row Intentionally left Blank													
1.	**Supporting Platform**															
1.1.	Operating system – Open source		Support													
1.2.	Operating system – COTS		License													
1.3.	Virtualisation software		License/ CPU	As required												
1.4.	Virtualisation Manager Software		License/ Support	1												
2.	**Core System Software Components**															

FORMAT 4B

Track 2: Phase 1 Middleware and Software

S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
2.1.	Web server		Core	4												
2.2.	Application Server		Core	4												
2.3.	BPM Software		Core	4												
2.4.	Document management system		Core	4												
2.5.	Database – OIOS		Core	4												

FORMAT 4B		Track 2: Phase 1 Middleware and Software														
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
2.6.	Database security – OIOS		Core	4												
2.7.	KMS Platform, discussion forum & Implementation		License	1												
2.8.	Help desk Tool – OIOS		License	1												
2.9.	Web conferencing tool (Helpdesk - multiple offices)		Host	10												
2.10	SIEM		License	As required												

FORMAT 4B			Track 2: Phase 1 Middleware and Software													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
2.11	Identity access and management (for 29,000 users -25% delivery)		License													
3.	**EMS Software**															
3.1.	Monitoring: IT Infrastructure (device based - OS Instances: Server OS, Virtualisation, Firewall, IPS, Storage)		Number	As required												
3.2.	Monitoring: OIOS Application Performance (Real User Monitoring, Diagnostics)		License	As required												

FORMAT 4B			Track 2: Phase 1 Middleware and Software													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
3.3.	Dashboard & Reporting (Events co-relation, Centralized Reporting)		License	As required												
3.4.	Service Desk (SLA monitoring, Incident Mgmt.)		License	As required												
3.5.	OIOS, IT Infrastructure Operational Analytics (Log Correlation & Analysis)		License	As required												
			Row Intentionally left Blank													
	Total Cost (In Numbers) Including Taxes															
	Total Cost (In Words) Including Taxes															

Timelines: 03 Months from Date of Agreement signing.

Note: Sl. No. 1-3: Delivery shall be limited to number of VMs planned for this Phase only

FORMAT 4C			Track 2: Phase 2 Middleware and Software													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
			Row Intentionally left Blank													
1.	**RDBMS Instance**															
1.1.	MySQL		Core	4												
1.2.	PostgreSQL		Core	4												
1.3.	MS SQL server		Core	4												
1.4.	DB2		Core	4												
1.5.	Oracle		Core	4												
Row Intentionally left Blank																
	Total Cost (In Numbers) Including Taxes															
	Total Cost (In Words) Including Taxes															

Note: Latest version of standard edition.

FORMAT 4D		Phase 3 Development Team					
S No	Resource Type	Quantity	Cost Per resource Per Month (Excluding Taxes)	Number of Months	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	C	D = A X B X C	E	F = D+(D*E/100)
All Amount to be quoted in INR							
1.	**Development Team**						
1.1.	Project Manager	1		18			
1.2.	Scrum Master	3		18			
1.3.	Enterprise Solution Architect	1		9			
1.4.	Security Architect	1		6			
1.5.	QC Expert	1		18			
1.6.	Business Analyst	3		6			
1.7.	Developers / Sr Developers	15		9			
1.8.	UX/ UI Designer	3		18			
1.9.	Test Lead	1		18			
1.10.	Tester	3		18			
1.11.	Data Preparation / Migration Expert	1		12			
1.12.	Database Administrator	1		12			
1.13.	System Administrator	1		18			

FORMAT 4D		Phase 3 Development Team					
S No	Resource Type	Quantity	Cost Per resource Per Month (Excluding Taxes)	Number of Months	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	C	D = A X B X C	E	F = D+(D*E/100)
All Amount to be quoted in INR							
Row Intentionally left Blank							
	Total Cost (In Numbers) Including Taxes						
	Total Cost (In Words) Including Taxes						

Note: For the above format, please indicate cost per resource per month as of 1st January 2020, and do NOT include any escalation in the table. Escalation for labour cost @ 8 per cent per annum on 1st January of each succeeding year will be separately provided for and paid for by IA&AD.

OIOS Phase 3 should be quoted on the basis of offsite deployment in this table. Onsite premium, if any, for onsite deployment of the entire development team in IA&AD premises, should be quoted in percentage terms.

FORMAT 4E	OIOS Cloud Development Environment to PDC Migration Cost				
S No	Components Name	Unit	Total Cost (Excluding Taxes)	Taxes %	Total Cost (Inclusive of Taxes)
			A	B	C = A + (A*B/100)
All Amount to be quoted in INR					
A	**Development environment Migration**	Lumpsum			
B	**Network reconfiguration and connectivity with PDC**	Lumpsum			
Row Intentionally left Blank					
C	***Total Cost (In Numbers) Including Taxes***				
	Total Cost (In Words) Including Taxes				

Format 5. Track 3: Setting Up of PDC and DRC and Backup Sites at 2 IA&AD offices

FORMAT 5A			Track 3: Phase 1 - Setting Up of PDC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
1.	**Hardware components**															
1.1.	Blade server chassis		Number	1												
1.2.	Blade Servers with 2X16 cores (Total 96 Cores)		Number	3												
1.3.	KVM Switch		Number	2												
1.4.	SAN storage 40 TB Usable		License/ Support	1												
1.5.	Racks		Number	As required												
1.6.	SAN Switch 24 Port		Number	2												

FORMAT 5A		Track 3: Phase 1 - Setting Up of PDC														
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
1.7.	Access switch 10G		Number	4												
1.8.	Structured Cabling within DC (Cat 6 A)		Job	1												
Row Intentionally left Blank																
2.	**Security**															
2.1.	Firewall Next Generation with SSL VPN (1 GBPS cumulative throughput including 7.2, 7.3 and 7.4)		Number	2												
2.2.	IPS		No	2												
2.3.	Application Security		Subscription/Year	2												
2.4.	URL filtering		Subscription/Year	2												
2.5.	Anti-APT Solution with sand-boxing		Subscription/Year	1												

FORMAT 5A			Track 3: Phase 1 - Setting Up of PDC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
2.6.	Web application firewall		No	2												
2.7.	DLP (System administrators console)		License	As required												
2.8.	HIPS		License	As required												
2.9.	Privilege Management of System Administrator (VMs, Physical Servers, Storage)		LIC / VM	As required												
2.10	Database Activity Monitoring		License	As required												
2.11	HSM		Number	1												
2.12	Anti-Virus – malware and Anti-Spam (for Server		Subscription/Year	As required												

FORMAT 5A			Track 3: Phase 1 - Setting Up of PDC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
	& System administration OS)															
Row Intentionally left Blank																
3.	**Backup Site 1/NLDC**															
3.1.	SAN (SAS based, 10TB usable capacity, expendable to 20TB usable)		Number	1												
3.2.	UPS (To support above SAN, with 30 min power backup)		Number	1												
Row Intentionally left Blank																
4.	**Lease line provisioning**															
4.1.	PDC to Backup Site 1/NLDC		Quarter	6												

FORMAT 5A			Track 3: Phase 1 - Setting Up of PDC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
4.2.	PDC to NICNET Gateway 1		Quarter	6												
Row Intentionally left Blank																
5.	Data Center Space Rental costs		Quarter	6												
Row Intentionally left Blank																
	Total Cost (In Numbers) Including Taxes															
	Total Cost (In Words) Including Taxes															

Note:

1. <u>**Timelines:** 03 Months from Date of Agreement signing.</u>
2. DMZ, MZ segregation shall be done using Firewall.
3. A separate management zone shall be created for deployment of Management and Monitoring Solution/ tools, using Access switch

FORMAT 5B			Track 3: Phase 2 - Setting Up of PDC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
1.	**Hardware components**															
1.1.	Blade Servers with 2X16 cores		Number	7												
Row Intentionally left Blank																
2.	**Supporting Platform**															
2.1.	Operating system – Open source		Support													
2.2.	Operating system - COTS		License/													
2.3.	Virtualisation software		License/ CPU	As required												
Row Intentionally left Blank																

FORMAT 5B			Track 3: Phase 2 - Setting Up of PDC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
3.	**Core System Software Components**															
3.1.	Web server		Core	4												
3.2.	Application Server		Core	4												
3.3.	BPM Software		Core	4												
3.4.	Document management system		Core	4												
3.5.	Database – OIOS		Core	12												
3.6.	Database security - OIOS		Core	12												
3.7.	Database Administration Software Tool for DBA		User License	10												
3.8.	GIS Server		Core	8												
Row Intentionally left Blank																

FORMAT 5B			Track 3: Phase 2 - Setting Up of PDC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
	Total Cost (In Numbers) Including Taxes															
	Total Cost (In Words) Including Taxes															

FORMAT 5C			Track 3: Phase 2 - Setting Up of DRC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
1.	**Hardware components**															
1.1.	Blade server chassis		Number	1												
1.2.	Blade Servers with 2X16 cores (Total 128 Cores)		Number	4												
1.3.	KVM Switch		Number	2												
1.4.	SAN storage 40 TB Usable		License/ Support	1												
1.5.	Racks		Number	As required												
1.6.	SAN Switch 24 Port		Number	2												
1.7.	Access switch 10G		Number	4												
1.8.	Structured Cabling within DC (Cat 6 A)		Job	1												

FORMAT 5C			Track 3: Phase 2 - Setting Up of DRC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
Row Intentionally left Blank																
2.	**Security**															
2.1.	Firewall Next Generation with SSL VPN (1 GBPS cumulative throughput including 7.2, 7.3 and 7.4)		Number	2												
2.2.	IPS		No	2												
2.3.	Application Security		Subscription/Year	2												
2.4.	URL filtering		Subscription/Year	2												
2.5.	Anti-APT Solution with sand-boxing		Subscription/Year	1												
2.6.	Web application firewall		No	2												

FORMAT 5C			Track 3: Phase 2 - Setting Up of DRC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
2.7.	DLP (System administrators console)		License	As required												
2.8.	HIPS		License	As required												
2.9.	Privilege Management of System Administrator (VMs, Physical Servers, Storage)		LIC / VM	As required												
2.10	Database Activity Monitoring		License	As required												
2.11	HSM		Number	1												
2.12	Anti-Virus – malware and Anti-Spam (for Server & System administration OS)		Subscription/Year	As required												

FORMAT 5C			Track 3: Phase 2 - Setting Up of DRC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
Row Intentionally left Blank																
3.	**Core System Software Components**															
3.1.	Site Recovery Software		License/DR	1												
3.2.	Web server		Core													
3.3.	Application Server		Core													
3.4.	BPM Software		Core													
3.5.	Document management system		Core													
3.6.	Database – OIOS		Core													
3.7.	Database security - OIOS		Core													
3.8.	Identity access and management		License													
3.9.	GIS Server		Core													

FORMAT 5C			Track 3: Phase 2 - Setting Up of DRC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
Row Intentionally left Blank																
4.	**Backup Site/NLDC**															
4.1.	SAN (SAS based, 10TB usable capacity, expendable to 20TB usable)		Number	2												
4.2.	UPS (To support above SAN, with 30 min power backup)		Number	2												
Row Intentionally left Blank																
5.	**Lease line provisioning**															
5.1.	Leased line between PDC, DRC of 50 Mbps		Quarter	6												
5.2.	PDC to Backup Site 2/NLDC		Quarter	6												

FORMAT 5C			Track 3: Phase 2 - Setting Up of DRC													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
5.3.	DRC to NICNET Gateway 2		Quarter	6												
Row Intentionally left Blank																
6.	DRC Space Rental Costs		Quarter	6												
Row Intentionally left Blank																
	Total Cost (In Numbers) Including Taxes															
	Total Cost (In Words) Including Taxes															

Note: It may be noted that there is no minimum BoM for sl no 3,4; however SI need to put necessary details as per solution and SLA.

Format 6. Track 4: Centralized Helpdesk Set Up and Operations

FORMAT 6		Centralized Helpdesk Resource				
S No	Resource Type	Indicative Person Months	Cost Per resource Per Month (Excluding Taxes)	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	C = A X B	D	E = C+(C*D/100)
1.	Application Support Manager	84				
2.	Manager - L1 and L2	72				
3.	Analyst - L1	168				
4.	Analyst - L2	156				
		Row Intentionally left Blank				
	Total Cost (In Numbers) Including Taxes					
	Total Cost (In Words) Including Taxes					

Refer Vol 1 centralized Helpdesk. This is a rate card matrix, and the number of resources can be adjusted upwards or downwards with prior notice by IA&AD.

Note 1: For the above format, please indicate cost per resource per month as of 1^{st} January 2020, and do NOT include any escalation in the table. Escalation @ 8 per cent per annum on 1^{st} January of each succeeding year will be separately provided for and paid for by IA&AD.

Note 2: OIOS Phase 2 should be quoted on the basis of offsite deployment in this table. Onsite premium, if any, for onsite deployment of the entire development team in IA&AD premises, should be quoted in percentage terms.

Format 7. Track 5: Training Cost

FORMAT 7		Training Cost (Inclusive of taxes)				
S No	Resource Type	Quantity/ Batch	Unit Cost Per training (Excluding Taxes)	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	C = A X B	D	E = C+(C*D/100)
All Amount to be quoted in INR						
1.	Agile Methodology Training	2				
2.	Toolchain Training	2				
3.	Training on the functional help desk tool	3				
4.	Application Training Phase 1	21				
5.	Application Training Phase 2	21				
6.	OIOS System Admin Training	3				
7.	Designing of MIS Reports/ dashboards	21				
8.	UAT Training Phase 1	9				
9.	UAT Training Phase 2	18				
Row Intentionally left Blank						
	Total Cost (In Numbers) Including Taxes					
	Total Cost (In Words) Including Taxes					

Note: Training Infrastructure and Location as indicated in Volume I.

Format 8. Track 6: Operations and Maintenance Cost

FORMAT 8		Track 6: Operation and Maintenance Cost												
S No	Resource Type	Qty	Cost / Resource / year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	Y1=AXB	Y2= AXB	Y3= AXB	Y4= AXB	Y5= AXB	Y6= AXB	Y7= AXB	C = Y1+Y2+Y3+ Y4+Y5+Y6+ Y7	D	E = C+(C*D/100)
All Amount to be quoted in INR													
1.	**Operation & Maintenance**												
1.1	Operations Manager	1											
1.2	Application Support Engineer	1											
1.3	Developer/ Sr. Developer	2											
1.4	Tester	1											

FORMAT 8

Track 6: Operation and Maintenance Cost

S No	Resource Type	Qty	Cost / Resource / year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	Y1=AXB	Y2=AXB	Y3=AXB	Y4=AXB	Y5=AXB	Y6=AXB	Y7=AXB	C = Y1+Y2+Y3+Y4+Y5+Y6+Y7	D	E = C+(C*D/100)
1.5	Database administrator	2											
1.6	System Administrator	2											
1.7	Infrastructure Manager	1											
1.8	Analyst – BCP and DR	3											
2.	**Security Administration**												
2.1	Security Manager	1											
2.2	Analyst (Application & Database Security)	3											

FORMAT 8	**Track 6: Operation and Maintenance Cost**												
S No	**Resource Type**	**Qty**	**Cost / Resource / year**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Total Cost (Excluding Taxes)**	**Tax %**	**Total Cost of Ownership (Including Taxes)**
		A	**B**	**Y1=AXB**	**Y2= AXB**	**Y3= AXB**	**Y4= AXB**	**Y5= AXB**	**Y6= AXB**	**Y7= AXB**	**C = Y1+Y2+Y3+Y4+Y5+Y6+Y7**	**D**	**E = C+(C*D/100)**
Row Intentionally left Blank													
	Total Cost (In Numbers) Including Taxes												
	Total Cost (In Words) Including Taxes												

Note:

- ***For the above format, please indicate cost per resource per month as of 1st January 2020, and do NOT include any cost escalation in the table. Escalation for labour cost @ 8 per cent per annum on 1st January of each succeeding year will be separately provided for and paid for by IA&AD.***
- ***Rates should be quoted, assuming that the O&M team is offsite. Please indicate separately onsite premium, if any, in percentage, if IA&AD decides that the O&M Team is to be located onsite on IA&AD premises.***
- Bidder to update Quantity as per the proposed O&M team in their Technical Proposal

Format 9. Compliance Sheet for Financial Proposal

S No	Basic Requirement	Documents Required	Provided	Reference & Page Number
1.	Covering Letter	As per Appendix II, Format 1	Yes / No	
2.	Financial Bid – Total Commercial Quote	Appendix II – Format 2	Yes / No	
3.	Financial Bid	Appendix II – Format 3 to Format 8	Yes / No	

Appendix III. Template for PBG and Integrity Pact

Format 1. Performance Bank Guarantee

PERFORMANCE SECURITY:

To: <Location, Date>

<Name>

<Designation>

<Address>

<Phone Nos.>

<email id>

Whereas, <<name of the supplier and address>> (hereinafter called "the Bidder") has undertaken, in pursuance of contract no. <Insert Contract No.> dated. <Date> to provide Implementation services for Implementation of One IAAD and One System to Comptroller and Auditor General if India (hereinafter called "the beneficiary")

And whereas it has been stipulated by in the said contract that the Bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract;

And whereas we, <Name of Bank> a banking company incorporated and having its head /registered office at <Address of Registered Office> and having one of its office at <Address of Local Office> have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of Rs.<Insert Value> (Rupees <Insert Value in Words> only) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of Rs. <Insert Value> (Rupees <Insert Value in Words> only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the Bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you and the

Bidder shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

This Guarantee shall be valid until <<Insert Date>>)

Notwithstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed Rs. <Insert Value> (Rupees <Insert Value in Words> only).

II. This bank guarantee shall be valid up to <Insert Expiry Date>)

It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before <Insert Expiry Date>) failing which our liability under the guarantee will automatically cease.

Format 2. Integrity Pact

PRE-CONTRACT INTEGRITY PACT

General

1. Whereas CA&G, hereinafter referred to as Purchaser and the first party, proposes to implement Project "Implementation of One IAAD One System", hereinafter referred to as Project, and M/s ___________________________________, represented by, ________________________ << Designation>> (which term, unless expressly indicated by the contract, shall be deemed to include its successors and its assignees), hereinafter referred to as the Bidder/Seller and the second party, is willing to offer/has offered IA&AD

2. Whereas the Bidder is a private company/public company/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the Purchaser is IA&AD performing its duty on behalf of GoI.

Objectives

3. Now, therefore, the Purchaser and the Bidder agree to enter into this pre-contract agreement, hereinafter referred to as Integrity Pact, to avoid all forms of corruption by following a system that is fair, transparent and free from any influence / unprejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:

   a. Enabling the Purchaser to implement the desired "Implementation of One IAAD One System" a competitive price in conformity with the defined specifications of the Services by avoiding the high cost and the distortionary impact of corruption on public procurement, and

   b. Enabling bidders to abstain from bribing or any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also refrain from bribing and other corrupt practices and the Purchaser will commit to prevent corruption, in any form, by their officials by following transparent procedures

Commitments of the Buyer

4. The Purchaser commits itself to the following:

   a. The Purchaser undertakes that no official of the Purchaser, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the Bidder, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the Contract.

b. The Purchaser will, during the pre-contract stage, treat all Bidders alike, and will provide to all Bidders the same information and will not provide any such information to any particular Bidder which could afford an advantage to that particular Bidder in comparison to other Bidders.

c. All the officials of the Purchaser will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

5. In case of any such preceding misconduct on the part of such official(s) is reported by the Bidder to the Purchaser with full and verifiable facts and the same is prima facie found to be correct by the Buyer, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the Purchaser and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the Buyer the proceedings under the contract would not be stalled.

Commitments of Bidders

6. The Bidder commits himself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of his bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commits himself to the following:

a. The Bidder will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Purchaser, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the Contract.

b. The Bidder further undertakes that he has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Purchaser or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the Contract or forbearing to show favour or dis-favor to any person in relation to the Contract or any other Contract with the Government.

c. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

d. The Bidder will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

e. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

f. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

g. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

h. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

i. The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract

j. The Bidder shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

7. Previous Transgression

a. The Bidder declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify bidder’s exclusion from the tender process.

b. If the Bidder makes incorrect statement on this subject, Bidder can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

8. Bank Guarantee

In the case of the successful bidder, a clause would also be incorporated in the Article pertaining to Performance Bank Guarantee in the Purchase Contract that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bank Guarantee in case of a decision by the Buyer to forfeit the same without assigning any reason for imposing sanction for violation of this pact.

9. Company Code of Conduct

Bidders are also advised to have a company code of conduct (clearly rejecting the use of bribes and other unethical behaviour) and a compliance program for the implementation of the code of conduct throughout the company.

10. Sanctions for Violation

a. Any breach of the aforesaid provisions by the Bidder or any one employed by him or acting on his behalf (whether with or without the knowledge of the Bidder) or the commission of any offence by the Bidder or any one employed by him or acting on his behalf, as defined in Chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act 1988 or any other act enacted for the prevention of corruption shall entitle the Purchaser to take all or any one of the following actions, wherever required:

   i. To immediately call off the pre-contract negotiations without assigning any reason or giving any compensation to the Bidder. However, the proceedings with the other Bidder(s) would continue.

   ii. To immediately cancel the contract, if already signed, without giving any compensation to the Bidder.

iii. The Performance Bank Guarantee / Other Guarantee shall stand forfeited either fully or partially, as decided by the Buyer and the Buyer shall not be required to assign any reason therefore

~~iv.~~ To recover all sums already paid by the Purchaser, in case of an Indian Bidder with interest thereon at 2% higher than the prevailing RBI Bank Rate.

v. To encash the advance bank guarantee and Performance-Bank Guarantee if furnished by the Bidder, in order to recover the payments, already made by the Buyer, along with interest.

vi. To cancel all or any other Contracts with the Bidder.

vii. To debar the Bidder from entering into any bid from the Government for India for a minimum period of five years, which may be further extended at the discretion of the Purchaser.

viii. To recover all sums paid in violation of this Pact by Bidder to any middleman or agent or broker with a view to securing the contract.

ix. If the Bidder or any employee of the Bidder or any person acting on behalf of the Bidder, either directly or indirectly, is closely related to any of the officers of the Purchaser, or alternatively, if any close relative of an officer of the Purchaser has financial interest/stake in the Bidder's firm, the same shall be disclosed by the Bidder at the time of filling the tender. Any failure to disclose the interest involved shall entitle the Buyer to rescind the contract without payment of any compensation to the Bidder.

x. The term 'close relative' for this purpose would mean spouse whether residing with the Government servant or not, but not include a spouse separated from the Government servant by a decree or order of a competent court; son or daughter or step son or step daughter and wholly dependent upon Government servant, but does not include a child or step child who is no longer in any way dependent upon the Government servant or of whose custody the Government servant has been deprived of by or under any law; any other person related, whether by blood or marriage, to the Government servant or to the Government servant's wife or husband and wholly dependent upon Government servant.

xi. The Bidder shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the Purchaser, and if he does so, the Purchaser shall be entitled forthwith to rescind the contract and all other contracts with the Bidder. The Bidder shall be liable to pay compensation for any loss or damage to the Buyer resulting from such rescission and the Buyer shall be entitled to deduct the amount so payable from the money(s) due to the Bidder.

xii. In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the Buyer with the Bidder, the same shall not be opened.

b. The decision of the Purchaser to the effect that a breach of the provisions of this Integrity Pact has been committed by the Bidder shall be final and binding on the Bidder, however, the Bidder can approach the monitor(s) appointed for the purposes of this Pact.

11. Fall Clause

a. The Bidder undertakes that he has not supplied/is not supplying the similar systems or subsystems at a price lower than that offered in the present bid in last 2 Years (from the date of bid submission) in respect of any other of any other project of similar size Ministry/Department of the Government of India and if it is found at any stage that the similar system of sub-system was supplied by the Bidder to any other Ministry / Department of the Government of India at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the Bidder to the Purchaser, if the contract has already been concluded.

b. The Bidder shall accord the most favoured customer treatment to the buyer in respect of all matters pertaining to the present case

12. IA&AD **Examination of Book of Records**

In case of any allegation of violation of any provisions of this Integrity Pact or payment of commission, the Purchaser or its agencies shall be entitled to examine the Books of Accounts of the Bidder and the Bidder shall provide necessary information of the relevant financial documents in English and shall extend all possible help for the purpose of such examination.

13. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the Purchaser i.e. New Delhi.

14. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

15. Validity

The validity of this Integrity Pact shall be from date of its signing and extend up to 5 years or the complete execution of the contract to the satisfaction of both the Purchaser and the Bidder/Seller, whichever is later.

Should one or several provisions of this pact turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

The Parties hereby sign this Integrity Pact at ___________ on ______________.

IA&AD

PURCHASER   BIDDER

Witness

1.   1.

2.   3.

Comptroller and Auditor General of India

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Request for Proposal

`Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

‘One IA&AD One System’ (OIOS) Project

VOLUME - III

Reference Number: 51-ISW/2019-‘One IA&AD One System’ Project

Disclaimer

The information contained in this Request for Proposal document (“RFP”) or subsequently provided to Bidders, whether verbally or in documentary or any other form by or on behalf of Comptroller & Auditor General of India (C&AG), or any of its employees or advisors, is provided to Bidders on the Terms and Conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is neither an offer nor an invitation by C&AG to the prospective Bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in the formulation of their Proposals pursuant to this RFP.

This RFP may not be appropriate for all companies, and it is not possible for C&AG, its employees or advisers to consider the objectives, technical expertise and particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP, may not be complete, accurate, adequate or correct. Each bidder should therefore conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments and information contained in this RFP and obtain independent advice from appropriate sources.

Information provided in this RFP to the Bidders is on a wide range of matters, some of which depend upon interpretation of facts. The information given is not an exhaustive account of requirements and should not be regarded as a complete or authoritative statement of facts. The specifications laid out in this RFP are indicated as the minimum requirements whereas the bidders are expected to focus on the objectives of the project and formulate their solution offerings in a manner that enables achieving those objectives in letter as well as spirit.

C&AG accepts no responsibility for the accuracy or otherwise for any interpretation or opinion expressed herein. C&AG, its employees and advisors make no representation or warranty and shall have no liability to any person including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, reliability or completeness of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process.

Page Intentionally Left Blank

Contents

MASTER SERVICES AGREEMENT

THIS MASTER SERVICE AGREEMENT ("Agreement") is made on this the <***> day of <***> 20… at

<***>, India.

BETWEEN

-- having its office at -----------------------------------

------------------------------ India hereinafter referred to as 'Purchaser' / 'Purchaser' or ' ', which

expression shall, unless the context otherwise requires, include its permitted successors and assigns);

AND

<***>, a Company incorporated under the Companies Act, 1956 or Companies Act, 2013 or limited liability partnership (LLP) under LLP Act, 2008, having its registered office at <***> (hereinafter referred to as 'the Implementation Agency/IA' which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as the 'Parties' and individually as a 'Party'.

WHEREAS:

1. The purchaser is desirous to implement a customized end-to-end IT system for the Indian Audit and Accounts Department viz. One IAAD one system.

2. In furtherance of the same, the purchaser undertook the selection of a suitable Implementation Agency through a competitive bidding process for implementing the Project and in this behalf issued Request for Proposal (RFP) dated <***> .

3. The successful bidder has been selected as the Implementation Agency on the basis of the bid response set out as **Annexure D** of this Agreement, to undertake the Project of the design, development and implementation of the solution, its roll out and sustained operations.

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1. Definitions

Terms and expressions used in this Agreement (including the Introduction) shall have the meanings set out below:

Term	Meaning
Adverse Effect	means material adverse effect on a) the ability of the Implementation Agency to exercise any of its rights or perform/discharge any of its duties/obligations under and in accordance with the provisions of this Agreement and/or b) the legal validity, binding nature or enforceability of this Agreement;
Agreement	means this Master Services Agreement, Service Level Agreement and Non-Disclosure Agreement together with all Articles, Annexures, Schedules and the contents and specifications of the RFP;
Applicable Law(s)	means any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project;
Assets	shall have the same meaning ascribed to it in Clause 10.1 (a)
Software	means the software designed, developed / customized, tested and deployed by the Implementation Agency for the purposes of the Project and includes the source code (in case of Bespoke development) along with associated documentation, which is the work product of the development efforts involved in the Project and the improvements and enhancements effected during the term of the Project, but does not include the third party software products (including the COTS products used for the product),

Term	Meaning
	proprietary software components and tools deployed by the Implementation Agency;
Bespoke Development	Bespoke development means development of custom-built software for One IAAD One System Project for Comptroller and Auditor General of India.
Business Hours	Shall mean the working time for Purchaser users which is 9:00 AM to 6:00 PM. Again for Web Server and other components which enable successful usage of web portals of the Purchaser the working time should be considered as 24 hours for all the days of the week. It is desired that IT maintenance, other batch processes (like backup) etc. should be planned so that such backend activities have minimum effect on the performance;
C&AG	means O/o Comptroller and Auditor General of India
Certificate(s) of Compliance	Shall have the same meaning ascribed to it in Clause 5.4;
Confidential Information	means all information including Purchaser Data (whether in written, oral, electronic or other format) which relates to the technical, financial and business affairs, dealers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how, plans, budgets, auditee data and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party in the course of or in connection with this Agreement (including without limitation such information received during negotiations, location visits and meetings in connection with this Agreement All such information in whatever form or mode of transmission, which is disclosed by a Party (the “Disclosing Party”) to any other Party (the “Recipient”) in connection with the Project during its implementation and which has been explicitly marked as “confidential”, or could be reasonably construed or inferred as being confidential or when disclosed orally, has been identified as confidential at the time of disclosure and has been confirmed and designated in writing within <15 days> from oral disclosure at the latest as confidential information by the Disclosing Party, is “Confidential Information”.

Term	Meaning
Control	means, in relation to any business entity, the power of a person to secure (i) by means of the holding of shares or the possession of voting power in or in relation to that or any other business entity, or (ii) by virtue of any powers conferred by the articles of association or other document regulating that or any other business entity, that the affairs of the first mentioned business entity are conducted in accordance with that person's wishes and in relation to a partnership, means the right to a share of more than one half of the assets, or of more than one half of the income, of the partnership;
COTS	Commercial off-the-shelf or commercially available off-the-shelf (COTS) products are packaged solutions which are adapted to satisfy the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions.
Deliverables	means the products, infrastructure and services agreed to be delivered by the Implementation Agency in pursuance of the agreement as defined more elaborately in the RFP, Implementation and the Maintenance phases and includes all documents related to the user manual, technical manual, design, process and operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related), inter alia payment and/or process related etc., source code and all its modifications or any other IP that may rightfully belong to the purchaser;
Proprietary Information	shall have the same meaning ascribed to it in Clause 19;
Effective Date	shall have the same meaning ascribed to it in Clause 4;
Purchaser Data	means all proprietary data of the department or its nominated agencies generated out of operations and transactions, documents all taxpayers data, all third party data including Auditee data and related information including but not restricted to user data which the Implementation Agency obtains, possesses or processes in the context of providing the Services to the users pursuant to this Agreement;
Final Acceptance Test	As explained in para 5.1.4 of volume 1

Term	Meaning
Force Majeure	shall have the same meaning ascribed to it in Clause 16.1;
Force Majeure Costs	shall have the same meaning ascribed to it in Clause 16.4 (b);
GoI	means the Government of India;
Go-Live	Shall have the same meaning ascribed to it in clause 23 of volume 1
Indemnifying Party	shall have the same meaning ascribed to it in Clause 15;
Indemnified Party	shall have the same meaning ascribed to it in Clause 15;
Intellectual Property Rights	means all rights in written designs and copyrights, moral rights, rights in databases and Bespoke Software / Pre-existing work including its upgradation systems and compilation rights (whether or not any of these are registered and including application for registration);
Escrow Agreement	Not Applicable
Insurance Cover	Implementation Agency shall purchase insurance for an appropriate amount to cover their liabilities on account of the follows: — Commercial General liability — Either professional indemnity or errors and omissions — Product liability
Additional Insurance	Not required
Material Breach	means a breach by either Party (Purchaser or Implementation Agency) of any of its obligations under this Agreement which has or is likely to have an Adverse Effect (such as OIOS/Auditee data breach, delays etc.) on the Project which such Party shall have failed to cure;
Required Deliverables	shall have the same meaning ascribed to it in Annexure F of this Agreement;
Parties	means Purchaser and Implementation Agency for the purposes of this Agreement and "***Party***" shall be interpreted accordingly;
Performance Guarantee	Means the guarantee provided by a Commercial Bank in favour of the Implementation Agency. The amount of Performance Security shall be 10% of the overall cost of the project. This performance security shall be

Term	Meaning
	valid till six months after the completion of the project i.e. **8 years** from the date of signing of contract or for such time as is required under this Agreement;
Planned Application Downtime	means the unavailability of the application services due to maintenance activities such as configuration changes, upgradation or changes to any supporting infrastructure wherein prior intimation (at least two working days in advance) of such planned outage shall be given and approval sought from the Purchaser as applicable;
Planned network outage	means the unavailability of the network services (to the extent of server side scope) due to infrastructure maintenance activities such as configuration changes, upgradation or changes to any supporting infrastructure. Prior intimation of such planned outage shall be given and approval sought from the Purchaser as applicable and shall be notified at least two working days in advance;
Project	means Pilot, Project Implementation (roll out) and Maintenance in terms of the Agreement;
Project Implementation	means Project Implementation as per the testing standards and acceptance criteria prescribed by Purchaser or its nominated agencies;
Project Timelines	shall have the same meaning ascribed to in section 9 of Volume 1
Providing Party	shall have the same meaning ascribed to it in Clause 12.5;
Receiving Party	shall have the same meaning ascribed to it in Clause 12.5;
Replacement Implementation Agency	means any third party that Purchaser or its nominated agencies appoint to replace the Implementation Agency upon expiry of the Term or termination of this Agreement to undertake the Services or part thereof;
Required Consents	means the consents, waivers, clearances and licenses to use Purchaser's Intellectual Property Rights, rights and other authorizations as may be required to be obtained for the software and other items that Purchaser or their nominated agencies are required to make available to Implementation Agency pursuant to this Agreement;
	means the services delivered to the Stakeholders of Purchaser or its nominated agencies, employees of Purchaser or its nominated agencies,

Term	Meaning
Services	and to professionals, using the tangible and intangible assets created, procured, installed, managed and operated by the Implementation Agency including the tools of information and communications technology and includes but is not limited to the list of services specified in Annexure B;
Service Level	means the level of service and other performance criteria which will apply to the Services delivered by the Implementation Agency;
SLA	means the Performance and Maintenance SLA executed as part of this Master Service Agreement;
Stakeholders	means the Purchaser or its nominated agencies,
Term	shall have the same meaning ascribed to it in Clause 3.1;
Third Party Systems	means systems (or any part thereof) in which the Intellectual Property Rights are not owned by the Purchaser or Implementation Agency and to which Implementation Agency has been granted a license to use and which are used in the provision of Services;
Unplanned Application Downtime	means the total time for all the instances where services in the software requirement specification document prepared by the Implementation Agency are not available for more than 5 consecutive minutes;
Network	in Purchaser users refers to all the IT assets installed by the Implementation Agency as part of the Project for networking;
Unplanned network outage	means the total time for all the instances where services in the scope of this agreement prepared by the Implementation Agency are not available for more than 5 consecutive minutes;
Application	means the software application developed as a part of scope of work set out in Clause 2.1(a)
Application Downtime	means the time for which user/s is not able to access the application. However, in calculating downtime, scheduled downtime (for example, backup time, batch processing time, routine maintenance time) would not be considered;

Term	Meaning
Network Uptime	Network Uptime refers to network availability between Purchaser's Head Quarters to Data center. "%Uptime" means ratio of 'up time' (in minutes) in a month to Total time in the month (in minutes) multiplied by 100;
Warranty / AMC Period	shall have the same meaning ascribed to it in Clause 20;
Safety and Security	shall have the same meaning ascribed to it in Clause 12.4;
Product Owner	An Officer of IAAD who is designated as the Product Owner (in agile parlance) for the development of OIOS.

1.2. Interpretation

In this Agreement, unless otherwise specified:

(a) references to Clauses, Sub-Clauses, Paragraphs, Schedules and Annexures are to clauses, sub-clauses, paragraphs, schedules and annexures to this Agreement;

(b) use of any gender includes the other genders;

(c) references to a '**company'** shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established;

(d) references to a '**person'** shall be construed so as to include any individual, firm, company, government, state or agency of a state, local or municipal authority or government body or any joint venture, association or partnership (whether or not having separate legal personality);

(e) a reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted;

(f) any reference to a 'day' (including within the phrase 'business day') shall mean a period of 24 hours running from midnight to midnight;

(g) references to a 'business day' shall be construed as a reference to a day (other than a Sunday) on which banks in the state of Delhi are generally open for business;

(h) references to times are to Indian Standard Time;

(i) a reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and

(j) all headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

(k) System integrator (SI) or Implementation Agency (IA) has been used for the same entity i.e. bidder selected for the project.

1.3. Measurement and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to two decimal places, with the third digit of five or above being rounded up and below five being rounded down except in money calculations where such amounts shall be rounded off to the nearest INR.

1.4. Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

(a) as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;

(b) as between the provisions of this Agreement and the Schedules/Annexures, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules/Annexures; and

(c) as between any value written in numerals and that in words, the value in words shall prevail.

1.5. Priority of documents

This Agreement, including its Schedules and Annexures, represents the entire agreement between the Parties as noted in this Clause. If in the event of a dispute as to the interpretation or meaning of this Agreement it should be necessary for the Parties to refer to documents forming part of the bidding process leading to this Agreement, then such documents shall be relied upon and interpreted in the following descending order of priority:

(a) This Agreement along with
(b) the SLA agreement,
(c) NDA agreement,
(d) Schedules and Annexures;
(e) the RFP along with subsequently issued corrigenda
(f) Technical and financial proposal submitted by the successful bidder, to the extent they along with subsequently issued clarifications furnished by the Implementation Agency in response to the RFP, to the extent they are not inconsistent with any terms of the RFP.

For the avoidance of doubt, it is expressly clarified that in the event of a conflict between this Agreement, Annexures / Schedules or the contents of the RFP, the terms of this Agreement shall prevail over the Annexures / Schedules and Annexures / Schedules shall prevail over the contents and specifications of the RFP.

2. Scope of the Project

The Implementation Agency shall be required to:

Develop / customize and implement One IAAD one system (OIOS); manage and provide technical support to the solution for the period of **7 years** from the date of Go-Live.

The roles and responsibilities of the Parties under this Agreement have been set out in detail as Annexure F of this Agreement.

For the avoidance of doubt, it is expressly clarified that this Agreement shall govern the provision of the contracted services under the SLA to the Purchaser and its nominated agencies. It is anticipated that new or renewal agreements may be undertaken by creating a separate SLA, with schedules and annexures as required, under this Agreement for each additional engagement.

2.1. Scope of work

Detailed Scope of Work for the selected bidder is as follows:

RFP Vol 1-

3. TERM AND DURATION OF THE AGREEMENT

This Agreement shall come into effect from date of signing (hereinafter the 'Effective Date') and shall continue till date of handing over and successful meeting of criteria defined under Exit Management Schedule II, subject to other ongoing and continuous obligations and liabilities on account of both the purchaser or it's nominated agencies and the Implementation Agency, unless terminated earlier (as per clause 14), in which case the contract will get terminated on fulfilment of all obligations mentioned as per clause 14 and Schedule-II.

4. Condition Precedent & Effective Date

4.1. Provisions to take effect upon fulfilment of Conditions Precedent

Subject to express terms to the contrary, the rights and obligations under this Agreement shall take effect only upon fulfilment of all the Conditions Precedent set out below. However, Purchaser or its nominated agencies may at any time at its sole discretion waive fully or partially any of the Conditions Precedent for the Implementation Agency and no such waiver shall affect or impair any right, power or remedy that the purchaser or its nominated agencies may otherwise have.

For the avoidance of doubt, it is expressly clarified that the obligations of the Parties (or its nominated agencies) under this Agreement shall commence from the fulfilment of the Conditions Precedent as set forth below.

4.2. a. Conditions Precedent of the Implementation Agency

The Implementation Agency shall be required to fulfil the Conditions Precedent in which is as follows:

(i) To provide a Performance Security/Guarantee, and other applicable guarantees/ payments within **15 days** of issue of Letter of Interest by the purchaser or on or before the day of singing the contract; and

(ii) Obtaining of all statutory and other approvals required for the performance of the Services under this Contract. This may include approvals/clearances, wherever applicable, that may be required for execution of this contract e.g. clearances from Government authorities for importing equipment, exemption of Tax/Duties/Levies, work permits/clearance, etc.

4.2. b. Conditions Precedent of the Purchaser

The Purchaser shall be required to fulfil the Conditions Precedents which are as follows:

i. Signing of Agreement with the Implementation Agency

ii. Providing required physical infrastructure for the project team(s)

iii. Necessary clearances associated with the execution of the project, unless specified to be performed by the IA

4.3. Extension of time for fulfilment of Conditions Precedent

The Parties may, by mutual agreement extend the time for fulfilling the Conditions Precedent and the Term of this Agreement.

4.4. Non-fulfilment of the Implementation Agency's Conditions Precedent

(a) In the event that any of the Conditions Precedent of the Implementation Agency have not been fulfilled within 15 days of signing of this Agreement and the same have not been waived fully or partially by the Purchaser or its nominated agencies, this Agreement shall cease to exist or the Purchaser may exercise the option to impose SLA where applicable for such delay.

(b) In the event that the Agreement fails to come into effect on account of non-fulfilment of the Implementation Agency's Conditions Precedent, the Purchaser or its nominated agencies shall not be liable in any manner whatsoever to the Implementation Agency and the Purchaser shall forthwith forfeit the Earnest Money Deposit.

(c) In the event that possession of any of the Purchaser or its nominated agencies facilities has been delivered to the Implementation Agency prior to the fulfilment of the Conditions Precedent, upon the termination of this Agreement such shall immediately revert to Purchaser or its nominated agencies, free and clear from any encumbrances or claims.

5. Obligations under the SLA

1) The SLA shall be a separate contract in respect of this Agreement and shall be entered into concurrently with this Agreement between Purchaser and Implementation Agency;

2) In relation to any future SLA entered into between the Parties; each of the Parties shall observe and perform the obligations set out herein.

3) **Change of Control:**

(a) In the event of a change of control of the Implementation Agency during the Term, the Implementation Agency shall promptly notify the Purchaser and/or its nominated agencies of the same in the format set out as Annexure A of this Agreement.

(b) In the event that the net worth of the surviving entity is less than that of Implementation Agency prior to the change of control, the Purchaser or its nominated agencies may within 30 days of becoming aware of such change in control, require a replacement of existing Performance Guarantee furnished by the Implementation Agency from a guarantor acceptable to the Purchaser or its nominated agencies (which shall not be the Implementation Agency or any of its associated entities).

(c) If such a guarantee is not furnished within 30 days of the Purchaser or its nominated agencies requiring the replacement, the Purchaser may exercise its right to terminate the SLA and/ or this Agreement within a further 30 days by written notice, to become effective as specified in such notice.

(d) Pursuant to termination, the effects of termination as set out in Clause 14 of this Agreement shall follow.

For the avoidance of doubt, it is expressly clarified that the internal reorganization of the Implementation Agency shall not be deemed an event of a change of control for purposes of this Clause unless the surviving entity is of less net worth than the predecessor entity.

4) **Final testing and certification**

The Project shall be governed by the mechanism of final acceptance testing and certification to be put into place by the Purchaser and Implementation Agency as under:

(a) Final testing and certification criteria will lay down a set of guidelines following internationally accepted norms and standards for testing and certification for all aspects of project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub- systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to compliance with SLA metrics, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and this Agreement;

(b) Final testing and certification criteria will be finalized from the development stage to ensure that the guidelines are being followed and to avoid large scale modifications pursuant to testing done after the application is fully developed;

(c) Final testing and certification criteria will consider conducting specific tests on the software, hardware, networking, security and all other aspects;

(d) Final testing and certification criteria (in parlance with section 5.1.4 of volume 1) will establish appropriate processes for notifying the Implementation Agency of any deviations from the norms, standards or guidelines at the earliest instance after taking cognizance of the same to enable the Implementation Agency to take corrective action; etc. in

5) The Parties shall each ensure that the range of the Services under the SLA shall not be varied, reduced or increased except with the prior written agreement between the Purchaser and Implementation Agency in accordance with the Change Control Schedule set out in Schedule I of this Agreement. Save for the express terms of the Terms of Payment Schedule set out as Schedule V of this Agreement, Purchaser or its nominated

agencies and its users may purchase any particular category of Services that may become necessary as per the Change Control Schedule set out in Schedule I of this Agreement, without the need to go for a separate procurement process.

6. Representations and Warranties

6.1. Representations and warranties of the Implementation Agency

The Implementation Agency represents and warrants to the Purchaser or its nominated agencies that:

(a) it is duly organized and validly existing under the laws of India, and has full power and authority to execute and perform its obligations under this Agreement and other agreements and to carry out the transactions contemplated hereby;

(b) It possesses necessary professional skills, human and technical resources to deliver the services it has offered to provide on the terms and conditions set forth in this Agreement.;

(c) It confirms that there is no conflict of interest on account of executing this project to the satisfaction of the purchaser;

(d) it has taken all necessary corporate and other actions under laws applicable to its business to authorize the execution and delivery of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;

(e) from the Effective Date, it will have the financial standing and capacity to undertake the Project in accordance with the terms of this Agreement. If the IA encounters adverse changes to its financial condition that affect service delivery, then it needs to notify the purchaser immediately;

(f) in providing the Services, it shall use reasonable endeavours not to cause any unnecessary disruption to Purchaser's normal business operations

(g) it undertakes to complete the project and handover the same to the purchaser without any encumbrance on the purchaser or whatsoever;

(h) this Agreement has been duly executed by it and constitutes a legal, valid and binding obligation, enforceable against it in accordance with the terms hereof, and its obligations under this Agreement shall be legally valid, binding and enforceable against it in accordance with the terms hereof;

(i) the information furnished in the Implementation Agency’s response to the RFP and any subsequent clarification pertaining to the evaluation process, furnished on or before the date of this Agreement is to the best of its knowledge and belief true and accurate in all material respects as at the date of this Agreement;

(j) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default by any of the terms of its Memorandum and Articles of Association or any Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

(k) there are no material actions, suits, proceedings, or investigations pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform any of its material obligations under this Agreement;

(l) it has no knowledge of any violation or default with respect to any order, writ, injunction or decree of any court or any legally binding order of any Government Instrumentality which may result in any Adverse Effect on its ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement;

(m) it has complied with Applicable Laws in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may have an Adverse Effect on its ability to perform its obligations under this Agreement;

(n) no representation or warranty by it contained herein or in any other document furnished by it to Purchaser or its nominated agencies in relation to the Required Consents contains or shall contain any untrue or misleading statement of material fact or omits or shall omit to state a material fact necessary to make such representation or warranty not misleading; and

(o) no sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for entering into this Agreement or for influencing or attempting to influence any officer or employee of Purchaser or its nominated agencies in connection therewith.

6.2. Representations and warranties of the Purchaser or its nominated agencies

Purchaser or its nominated agencies represent and warrant to the Implementation Agency that:

(a) it has full power and authority to execute, deliver and perform its obligations under this Agreement and to carry out the transactions contemplated herein and that it has taken all actions necessary to execute this Agreement, exercise its rights and perform its obligations, under this Agreement and carry out the transactions contemplated hereby;

(b) it has taken all necessary actions under Applicable Laws to authorize the execution, delivery and performance of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;

(c) it has the financial standing and capacity to perform its obligations under the Agreement;

(d) it is subject to the laws in India, and hereby expressly and irrevocably waives any immunity in any jurisdiction in respect of this Agreement or matters arising thereunder including any obligation, liability or responsibility hereunder;

(e) this Agreement has been duly executed by it and constitutes a legal, valid and binding obligation enforceable against it in accordance with the terms hereof and its obligations under this Agreement shall be legally valid, binding and enforceable against it in accordance with the terms thereof;

(f) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default under, or accelerate performance required by any of the Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

(g) there are no actions, suits or proceedings pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the default or breach of this

Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform its material (including any payment) obligations under this Agreement;

(h) it has no knowledge of any violation or default with respect to any order, writ, injunction or any decree of any court or any legally binding order of any Government Instrumentality which may result in any Adverse Effect on the Purchaser or its nominated agencies ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement;

(i) it has complied with Applicable Laws in all material respects;

(j) all information provided by it in the RFP in connection with the Project is, to the best of its knowledge and belief, true and accurate in all material respects; and

(k) upon the Implementation Agency performing the covenants herein, it shall not at any time during the term hereof, interfere with peaceful exercise of the rights and discharge of the obligations by the Implementation Agency, in accordance with this Agreement.

7. OBLIGATIONS OF THE PURCHASER OR ITS NOMINATED AGENCIES

Without prejudice to any other undertakings or obligations of the Purchaser or its nominated agencies under this Agreement, the Purchaser or its nominated agencies shall perform the following:

(a) To provide any support through personnel to test the system during the Term;

(b) To provide any support through personnel and/or test data during development, rollout, steady state operation, as well as, for any changes/enhancements in the system whenever required due to scope change that may arise due to business, delivery or statutory/regulatory reasons;

(c) To provide the data (including in electronic form wherever available) to be migrated.

(d) **Provide prompt Deliverable feedback:**

Within **15 working days** from the submission of a deliverable/SLA and performance reports, the purchaser shall provide a sign offs on the deliverable or its comments for changes.

In case the purchaser fails to respond and provide feedback on above stated submission, the deliverables or SLA and performance reports will be deemed accepted. Post **15 working days** there will be no rework of the said deliverable except, in case the purchaser has provided an alternate date for acceptance. Any subsequent rework post acceptance / deemed acceptance would form the subject of a formal change request under the provisions of this Agreement.

8. OBLIGATIONS OF THE IMPLEMENTATION AGENCY

1) It shall provide to the Purchaser or its nominated agencies, the Deliverables as set out in Annexure C of this Agreement.

2) It shall perform the Services as set out in Clause 2 of this Agreement and in a good and workmanlike manner commensurate with industry and technical standards which are generally in effect for international projects and innovations pursuant thereon similar to those contemplated by this Agreement, and so as to comply with the applicable Service Levels set out with this Agreement.

3) It shall ensure that the Services are being provided as per the Project Timelines set out in the RFP or as set by the purchaser after mutual discussion and sign off with Implementation Agency.

9. APPROVALS AND REQUIRED CONSENTS

1) The Parties shall cooperate to procure, maintain and observe all relevant and regulatory and governmental licenses, clearances and applicable approvals (hereinafter the "**Required Consents**") necessary for the Implementation Agency to provide the Services. The costs of such Approvals shall be borne by the Party normally responsible for such costs according to local custom and practice in the locations where the Services are to be provided.

2) In the event that any Required Consent is not obtained, the Implementation Agency and the Purchaser or its nominated agencies will co-operate with each other in achieving a reasonable alternative arrangement as soon as reasonably practicable for the Purchaser or its nominated agencies to continue to process its work with as minimal interruption to its business operations as is commercially reasonable until such Required Consent is obtained, provided that the Implementation Agency shall not be relieved of its obligations to provide the Services and to achieve the Service Levels until the Required Consents are obtained if and to the extent

that the Implementation Agency's obligations are not dependent upon such Required Consents.

10. USE OF ASSETS BY THE IMPLEMENTATION AGENCY

1) During the Term the Implementation Agency shall:

(a) take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components used for the Project and other facilities leased / owned / operated by the Implementation Agency exclusively in terms of ensuring their usability for the delivery of the Services as per this Agreement (hereinafter the "**Assets**") in proportion to their use and control of such Assets; and

(b) keep all the tangible Assets in as good and serviceable condition (reasonable wear and tear excepted) as at the date the Implementation Agency takes control of and/or first uses the Assets and during the entire Term of the Agreement.

(c) ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of the Assets and which are provided to the Implementation Agency will be followed by the Implementation Agency and any person who will be responsible for the use of the Assets;

(d) take such steps as may be properly recommended by the manufacturer of the Assets and notified to the Implementation Agency or as may, in the reasonable opinion of the Implementation Agency, be necessary to use the Assets in a safe manner;

(e) ensure that the Assets that are under the control of the Implementation Agency, are kept suitably housed and in conformity with Applicable Law;

(f) procure permission from the Purchaser or its nominated agencies and any persons duly authorized by them to enter any land or premises on which the Assets are for the time being sited so as to inspect the same, subject to any reasonable third party requirements;

(g) not knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to Applicable Law.

11. ACCESS TO THE PURCHASER OR ITS NOMINATED AGENCIES LOCATIONS

1) For so long as the Implementation Agency provides services to the Purchaser or its nominated agencies location, as the case may be, on a non-permanent basis and to the extent necessary, the Purchaser as the case may be or its nominated agencies shall, subject to compliance by the Implementation Agency with any safety and security guidelines which may be provided by the Purchaser as the case may be or its nominated agencies and notified to the Implementation Agency in writing, provide the Implementation Agency with:

   (a) reasonable access, in the same manner granted to the Purchaser or its nominated agencies employees, to the Purchaser as the case may be location twenty-four hours a day, seven days a week;

   (b) Reasonable work space, access to office equipment as mutually agreed and other related support services in such location other the Purchaser as the case may be location, if any, as may be reasonably necessary for the Implementation Agency to perform its obligations hereunder and under the SLA.

2) Reasonable access to locations, office equipment's and services shall be made available to the Implementation Agency in appropriate working condition (as per scope of work and the responsibilities defined in the tender) by the Purchaser as the case may be or its nominated agencies. The Implementation Agency agrees to ensure that its employees, agents and contractors shall not use the location, services and equipment referred to in RFP for the following purposes:

   (a) for the transmission of any material which is defamatory, offensive or abusive or of an obscene or menacing character; or

   (b) in a manner which constitutes a violation or infringement of the rights of any person, firm or company (including but not limited to rights of copyright or confidentiality).

3) The implementation agency is prohibited from using the provided space in a manner that shall contravene any extant law.

12. MANAGEMENT PHASE

12.1. Governance

The review and management process of this Agreement shall be carried out in accordance with the Governance Schedule set out in Schedule IV of this Agreement and shall cover all the management aspects of the Project.

12.2. Use of Services

a) The Purchaser as the case may be or its nominated agencies, will undertake and use the Services in accordance with any instructions or procedures as per the acceptance criteria as set out in the SLA or this Agreement or any agreement that may be entered into between the Parties from time to time;

b) The Purchaser as the case may be or its nominated agencies shall be responsible for the operation and use of the Deliverables resulting from the Services

12.3. Changes

Unless expressly dealt with elsewhere in this Agreement, any changes under or to this Agreement or under or to the SLA shall be dealt with in accordance with the Change Control Schedule set out in Schedule I of this Agreement.

12.4. Security and Safety

a) The Implementation Agency shall comply with the technical requirements of the relevant security, safety and other requirements specified in the Information Technology Act or Telegraph Act including the regulations issued by the Dept. of Telecommunication (wherever applicable), IT Security Manual of the Purchaser as specifically stated in the RFP and follow the industry standards related to safety and security (including those as stated in the RFP), insofar as it applies to the provision of the Services.

b) Either Parties to the SLA/Agreement shall use reasonable endeavours to report forthwith in writing to each other all identified attempts (whether successful or not) by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Purchaser as the case may be or any of their nominees data, facilities or Confidential Information.

c) The Implementation Agency shall upon request by the Purchaser as the case may be or their nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.

d) As per the provisions of the SLA or this Agreement, the Implementation Agency shall promptly report in writing to the Purchaser or its nominated agencies, any act or omission which they are aware that could have an adverse effect on the proper conduct of safety and information technology security at the facilities of Purchaser as the case may be.

e) The Implementation Agency shall ensure compliance to all extant laws regarding safety and security.

12.5. Cooperation

Except as otherwise provided elsewhere in this Agreement or the SLA, each Party ("***Providing Party***") to this Agreement or to the SLA undertakes promptly to provide the other Party ("***Receiving Party***") with all such information and co-operation which the Receiving Party reasonably requests, provided that such information and co-operation:

a) is reasonably required by the Receiving Party in order for it to comply with its obligations under this Agreement or the SLA;

b) cannot be construed to be Confidential Information; and

c) is capable of being provided by the Providing Party.

Further, each Party agrees to co-operate with the contractors and subcontractors of the other Party as reasonably requested in order to accomplish the purposes of this Agreement.

13. FINANCIAL MATTERS

13.1. Terms of Payment

a) In consideration of the Services and subject to the provisions of this Agreement and of the SLA, the Purchaser shall pay the Implementation Agency for the Services rendered in pursuance of this agreement, in accordance with the Terms of Payment Schedule set out as Schedule V of this Agreement.

b) Payments shall be subject to the application of liquidated damages (for period prior to "Go Live") or SLA penalties and its adjustments/corrections (for post "Go-Live")as may be provided for in the Agreement and the SLA from the relevant milestone(s)

c) Save and except as otherwise provided for herein or as agreed between the Parties in writing, the Purchaser shall not be required to make any payments in respect of the Services (or, without limitation to the foregoing, in respect of the Implementation Agency performance of any obligations under this Agreement or the SLA) other than those covered in Schedule V of this Agreement. For the avoidance of doubt, it is expressly clarified that the payments shall be deemed to include all ancillary and incidental costs and charges arising in the course of delivery of the Services including consultancy charges, infrastructure costs, project costs, implementation and management charges and all other related costs including taxes which are addressed in this Clause.

13.2. Invoicing and Settlement

a) Subject to the specific terms of the Agreement and the SLA, the Implementation Agency shall submit its invoices in accordance with the following principles:

i. The Purchaser shall be invoiced by the Implementation Agency for the Services. Generally and unless otherwise agreed in writing between the Parties or expressly set out in the SLA, the Implementation Agency shall raise an invoice as per Schedule V of this Agreement; and

ii. Any invoice presented in accordance with this Clause shall be in a form agreed with the Purchaser.

b) The Implementation Agency alone shall invoice all payments after receiving due approval of completion of payment milestone from the competent authority. Such invoices shall be accurate with all adjustments or changes in the terms of payment as stated in Schedule V of this Agreement. The Implementation Agency shall waive any charge for a Service that is not invoiced within six months after the end of the month in which the change relating to such Service is (i) authorized or (ii) incurred, whichever is later.

c) Payment shall be made within 60 days of the receipt of invoice along with supporting documents by the Purchaser subject to deduction of applicable liquidated damages (till "Go Live") or SLA penalties (post "Go Live") . The penalties are imposed on the vendor as per the SLA criteria specified in the SLA. In the event of delay in payment of undisputed amount beyond 60 days, Implementation Agency shall be entitled to a late payment interest of **RBI Bank rate** per annum from the date of completion of 60 days after submission of invoice. This interest is subject to a limit of 10% of the total contract value.

d) The Purchaser shall be entitled to delay or withhold payment of any invoice or part of it delivered by the Implementation Agency under Schedule V of this Agreement where the Purchaser disputes/withholds such invoice or part of it provided that such dispute is bona fide. The withheld amount shall be limited to that which is in dispute. The disputed / withheld amount shall be settled in accordance with the escalation procedure as set out in Schedule V of this Agreement. Any exercise by the Purchaser under this Clause shall not entitle the Implementation Agency to delay or withhold provision of the Services.

e) The Implementation Agency shall be solely responsible to make payments to its sub-contractors.

13.3. Tax

a) The Purchaser or its nominated agencies shall be responsible for withholding taxes from the amounts due and payable to the Implementation Agency wherever applicable. The Implementation Agency shall pay for all other taxes in connection with this Agreement, SLA, scope of work and any other engagement required to be undertaken as a part of this Agreement, including, but not limited to, property, sales, use, excise, value-added, goods and services, consumption and other similar taxes or duties.

b) The Purchaser or its nominated agencies shall provide Implementation Agency with the original tax receipt of any withholding taxes paid by Purchaser or its nominated agencies on payments under this Agreement. The Implementation Agency agrees to reimburse and hold the Purchaser or its nominated agencies harmless from any deficiency including penalties and interest relating to taxes that are its responsibility under this paragraph. For purposes of this Agreement, taxes shall include taxes incurred on transactions between and among the Purchaser or its nominated agencies, the Implementation Agency and third party subcontractors.

c) If, after the date of this Agreement, there is any change of rate of levy under the existing applicable laws of India with respect to taxes and duties, which are directly payable by the Purchaser for providing the goods and services i.e. service tax or any such other applicable tax from time to time, which increase or decreases the cost incurred by the Implementation Agency in performing the Services, then the remuneration and reimbursable expense otherwise payable to the Implementation Agency under this Agreement shall be increased or decreased accordingly by correspondence between the Parties hereto, and corresponding adjustments shall be made to the ceiling amounts specified in Schedule V. However, in case of any new or fresh tax or levy imposed after submission of the proposal the Implementation Agency shall be entitled to reimbursement on submission of proof of payment of such tax or levy.

d) The Parties shall cooperate to enable each Party to accurately determine its own tax liability and to minimize such liability to the extent legally permissible. In connection therewith, the Parties shall provide each other with the following:

   i. any resale certificates;

   ii. any relevant information regarding out-of-state or use of materials, equipment or services; and

   iii. any direct pay permits, exemption certificates or information reasonably requested by the other Party.

14. TERMINATION

14.1. FOR MATERIAL BREACH

a) In the event that either Party believes that the other Party is in Material Breach of its obligations under this Agreement, such aggrieved Party may terminate this Agreement upon giving a one month’s notice for curing the Material Breach to the other Party. In case the Material Breach continues, after the notice period, the Purchaser or Implementation Agency, as the case may be will have the option to terminate the Agreement. Any notice served pursuant to this Clause shall give reasonable details of the Material Breach, which could include the following events and the termination will become effective:

   i. If the Implementation Agency is not able to deliver the services as per the SLAs defined in RFP which translates into Material Breach, then the Purchaser may serve a 30 days written notice for curing this Material Breach. In case the Material Breach continues, after the expiry of such notice period, the Purchaser will have the option to terminate this Agreement. Further, the Purchaser may offer a reasonable opportunity to the Implementation Agency to explain the circumstances leading to such a breach.

b) The Purchaser may by giving a one month's written notice, terminate this Agreement if a change of control of the Implementation Agency has taken place. For the purposes of this Clause, in the case of Implementation Agency, change of control shall mean the events stated in Clause 5, and such notice shall become effective at the end of the notice period as set out in Clause 5.3 (c).

c) In the event that Implementation Agency undergoes such a change of control, Purchaser may, as an alternative to termination, require a full Performance Guarantee for the obligations of Implementation Agency by a guarantor acceptable to Purchaser or its nominated agencies. If such a guarantee is not furnished within 30 days of Purchaser's demand, the Purchaser may exercise its right to terminate this Agreement in accordance with this Clause by giving 15 days further written notice to the Implementation Agency.

d) The termination provisions set out in this Clause shall apply mutatis mutandis to the SLA.

14.2. Termination for Convenience

1) The Purchaser may at any time terminate the Contract for any reason by giving the IA a notice of termination that refers to this clause.

2) Upon receipt of the notice of termination under this clause, the IA shall either as soon as reasonably practical or upon the date specified in the notice of termination:

   a) cease all further work, except for such work as the Purchaser may specify in the notice of termination for the sole purpose of protecting that part of the System already executed, or any work required to leave the site and system in a clean and safe condition;

   b) terminate all subcontracts, except those to be assigned to the Purchaser pursuant to Clause 14.2.(I) (d) (ii) below;

   c) remove all IA's Equipment from the site, repatriate the IA's and its Subcontractors' personnel from the site, remove from the site any wreckage, rubbish, and debris of any kind;

   d) in addition, the IA shall:

      i. deliver to the Purchaser the parts of the System executed by the IA up to the date of termination;

      ii. to the extent legally possible, assign to the Purchaser all right, title, and benefit of the IA to the System, or Subsystem, as at the date of termination, and, as may be required by the Purchaser, in any subcontracts concluded between the IA and its Subcontractors;

iii. Deliver to the Purchaser all drawings, specifications, and other documents prepared by the IA or its Subcontractors as of the date of termination in connection with the System.

14.3. Effects of termination

a) In the event that Purchaser terminates this Agreement pursuant to failure on the part of the Implementation Agency to comply with the conditions as contained in this Clause and depending on the event of default, Performance Guarantee furnished by Implementation Agency may be forfeited.

b) Upon termination of this Agreement, the Parties will comply with the Exit Management Schedule set out as Schedule II of this Agreement.

c) In the event that Purchaser or the Implementation Agency terminates this Agreement, the compensation will be decided in accordance with the Terms of Payment Schedule set out as Schedule V of this Agreement.

d) Purchaser agrees to pay Implementation Agency for i) all charges for Services Implementation Agency provides and any Deliverables and/or system (or part thereof) Implementation Agency delivers through termination for convenience and any charges at the tendered rate, for extension period beyond termination as decided by the Nodal Agency as per Schedule 2, Clause 2.2 and ii) reimbursable expenses Implementation Agency pre closure termination.

e) If Purchaser terminates without cause, Purchaser also agrees to pay any applicable adjustment expenses to Implementation Agency incurs as a result of such termination (which Implementation Agency will take reasonable steps to mitigate.

f) In the event of termination of the Contract under 14.2, the Purchaser shall pay to the IA the following amounts:

i. the Contract Price, properly attributable to the parts of the System executed by the IA as of the date of termination;

ii. the costs reasonably incurred by the IA in the removal of the IA’s Equipment from the site and in the repatriation of the IA’s and its Subcontractors’ personnel;

iii. any amount to be paid by the IA to its Subcontractors in connection with the termination of any subcontracts, including any cancellation charges;

iv. costs incurred by the IA in protecting the System and leaving the site in a clean and safe condition pursuant to Clause 14.2; and

v. the cost of satisfying all other obligations, commitments, and claims that the IA may in good faith have undertaken with third parties in connection with the Contract and that are not covered by Clauses 14.3 (d) above.

14.4. Termination of this Agreement due to bankruptcy of Implementation Agency

The Purchaser may serve written notice on Implementation Agency at any time to terminate this Agreement with immediate effect in the event that the Implementation Agency reporting an apprehension of bankruptcy to the Purchaser or its nominated agencies.

15. INDEMNIFICATION & LIMITATION OF LIABILITY

1) Subject to Clause 15.4 below, Implementation Agency (the "Indemnifying Party") undertakes to indemnify, hold harmless the Purchaser (the "Indemnified Party") from and against all claims, liabilities, losses, expenses (including reasonable attorneys' fees), fines, penalties, taxes or damages (Collectively “Loss”) on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence or willful default in performance or non-performance under this Agreement.

2) If the Indemnified Party promptly notifies Indemnifying Party in writing of a third party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party.

3) Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by

   a. Indemnified Party’s misuse or modification of the Service;
   b. Indemnified Party’s failure to use corrections or enhancements made available by the Indemnifying Party;
   c. Indemnified Party’s use of the Service in combination with any product or information not owned or developed by Indemnifying Party;

However, if any service, information, direction, specification or materials provided by Indemnified Party or any third party contracted to it, is or likely to be held to be infringing, Indemnifying Party shall at its expense and option either

i. Procure the right for the Indemnified Party to continue using it

ii. Replace it with a non-infringing equivalent

iii. Modify it to make it non-infringing

The foregoing remedies constitute the Indemnified Party's sole and exclusive remedies and Indemnifying Party's entire liability with respect to infringement.

4) The indemnities set out in Clause 15 shall be subject to the following conditions:

i. the Indemnified Party as promptly as practicable informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;

ii. the Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the Defense of such claim including reasonable access to all relevant information, documentation and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such Defense;

iii. if the Indemnifying Party does not assume full control over the Defense of a claim as provided in this Article, the Indemnifying Party may participate in such Defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be included in Losses;

iv. the Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party;

v. all settlements of claims subject to indemnification under this Clause will:

vi. the Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favour of the Indemnified Party which are to be paid to it in connection with any such claim or proceedings;

vii. the Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings;

viii. in the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defenses of the Indemnified Party with respect to the claims to which such indemnification relates; and

ix. if a Party makes a claim under the indemnity set out under Clause 15.(A) above in respect of any particular Loss or Losses, then that Party shall not be entitled to make any further claim in respect of that Loss or Losses (including any claim for damages).

5) The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed the total contract value payable under this Agreement. The liability cap given under this Clause shall not be applicable to the indemnification obligations set out in Clause 15 and breach of Clause 12.4 and 17.

6) In no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) nor for any third party claims (other than those set-forth in Clause 15.(A)) even if it has been advised of their possible existence.

7) The allocations of liability in this Section 15 represent the agreed and bargained-for understanding of the parties and compensation for the Services reflects such allocations. Each Party has a duty to mitigate the damages and any amounts payable under an indemnity that would otherwise be recoverable from the other Party pursuant to this Agreement by taking appropriate and commercially reasonable actions to reduce or limit the amount of such damages or amounts.

16. FORCE MAJEURE

1) Definition of Force Majeure

“Force Majeure” shall mean any event beyond the reasonable control of the Purchaser or of the Supplier, as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected.

2) Force Majeure events

A Force Majeure shall include, without limitation, the following:

a) war, hostilities, or warlike operations (whether a state of war be declared or not), invasion, act of foreign enemy, and civil war;
b) Sabotage, embargo, import restriction, port congestion, force majeure ;
c) earthquake, landslide, volcanic activity, fire, flood or inundation, tidal wave, typhoon

or cyclone, hurricane, storm, lightning, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster;

1) If either party is prevented, hindered, or delayed from or in performing any of its obligations under the Contract by an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within fourteen (14) days after the occurrence of such event.

2) The party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract for so long as the relevant event of Force Majeure continues and to the extent that such party's performance is prevented, hindered, or delayed. The time for achieving Final Acceptance shall be extended.

3) The party or parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure upon its or their performance of the Contract and to fulfil its or their obligations under the Contract, but without prejudice to either party's right to terminate the Contract under Clause 16.

4) No delay or non-performance by either party to this Contract caused by the occurrence of any event of Force Majeure shall:

   a) constitute a default or breach of the Contract;
   b) give rise to any claim for damages or additional cost or expense occasioned by the delay or non-performance,

   if, and to the extent that, such delay or non-performance is caused by the occurrence of an event of Force Majeure.

5) If the performance of the Contract is substantially prevented, hindered, or delayed for a single period of more than sixty (60) days on account of one or more events of Force Majeure during the time period covered by the Contract, the parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract by giving a notice to the other.

6) In the event of termination pursuant to Clause 16, the rights and obligations of the Purchaser and the Supplier shall be as specified in the clause titled Termination.

7) Notwithstanding Clause 16.2.4, Force Majeure shall not apply to any obligation of the Purchaser to make payments to the Supplier under this Contract.

8) For the avoidance of doubt, it is expressly clarified that the failure on the part of the Implementation Agency under this Agreement or the SLA to implement any disaster contingency planning and back-up and other data safeguards in accordance with the terms of this Agreement or the SLA against natural disaster, fire, sabotage or other similar occurrence shall not be deemed to be a Force Majeure event. For the avoidance of doubt, it is further clarified that any negligence in performance of Services which directly causes any breach of security like hacking are not the forces of nature and hence would not be qualified under the definition of "Force Majeure". In so far as applicable to the performance of Services, The Service Provider will be solely responsible to complete the risk assessment and ensure implementation of adequate security hygiene, best practices, processes and technology to prevent any breach of security and any resulting liability therefrom (wherever applicable).

17. CONFIDENTIALITY

1) The Purchaser or its nominated agencies shall allow the Implementation Agency to review and utilize highly confidential public records and the Implementation Agency shall maintain the highest level of secrecy, confidentiality and privacy with regard thereto.

2) Additionally, the Implementation Agency shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities.

3) The Purchaser or its nominated agencies shall retain all rights to prevent, stop and if required take the necessary punitive action against the Implementation Agency regarding any forbidden disclosure.

4) The Implementation Agency shall ensure that all its employees, agents and sub-contractors involved in the project, execute individual non-disclosure agreements, which have been duly approved by the Purchaser with respect to this Project. The implementing agency may submit a declaration that it has obtained the NDA from its employees and sub-contractors.

   For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

   a) information already available in the public domain;
   b) information which has been developed independently by the Implementation Agency, independent of this project;

c) information which has been received from a third party who had the right to disclose the aforesaid information;

d) Information which has been disclosed to the public pursuant to a court order.

5) To the extent the Implementation Agency shares its confidential or proprietary information with the Purchaser for effective performance of the Services, the provisions of Clause 17.1, 17.2 and 17.3 shall apply mutatis mutandis on the Purchaser or its nominated agencies.

6) Any handover of confidential information needs to be maintained in a list, both by Purchaser & SI, containing at the very minimum, the name of provider, recipient, date of generation of the data, date of handing over of data, mode of information, purpose and signatures of both parties.

7) Notwithstanding anything to the contrary mentioned hereinabove, the Implementation Agency shall have the right to share the Letter of Intent / work order provided to it by the Purchaser in relation to this Agreement, with it's prospective purchasers solely for the purpose of and with the intent to evidence and support its work experience under this Agreement

18. AUDIT, ACCESS AND REPORTING

The Implementation Agency shall allow access to the Purchaser or its nominated agencies to all information which is in the possession or control of the Implementation Agency and which relates to the provision of the Services as set out in the Audit, Access and Reporting Schedule and which is reasonably required by the Purchaser to comply with the terms of the Audit, Access and Reporting Schedule set out as Schedule III of this Agreement.

19. INTELLECTUAL PROPERTY RIGHTS

1. **Products and fixes:**

   All products and related solutions and fixes provided pursuant to this Agreement shall be licensed according to the terms of the license agreement packaged with or otherwise applicable to such product, the ownership of which shall continue to vest with the product owner. Implementation Agency would be responsible for arranging any licenses associated with products.

“Product” means any computer code, web-based services, or materials comprising commercially released, pre-release or beta products (whether licensed for a fee or no charge) and any derivatives of the foregoing which are made available to Purchaser for license which is published by product owner or its affiliates, or a third party. “Fixes” means product fixes that are either released generally (such as commercial product service packs) or that are provided to you when performing services (such as workarounds, patches, bug fixes, beta fixes and beta builds) and any derivatives of the foregoing.

2. **Bespoke development:**

Subject to the provisions of Clause 19.C and 19.D below, upon payment, the IPR rights for any bespoke development done during the implementation of the project will lie exclusively with the Purchaser.

3. **Pre-existing work:**

All IPR including the source code and materials developed or otherwise obtained independently of the efforts of a Party under this Agreement (“pre-existing work”) including any enhancement or modification thereto shall remain the sole property of that Party. During the performance of the services for this agreement, each party grants to the other party (and their sub-contractors as necessary) a non-exclusive license to use, reproduce and modify any of its pre-existing work provided to the other party solely for the performance of such services for duration of the Term of this Agreement. Except as may be otherwise explicitly agreed to in a statement of services, upon payment in full, the Implementation Agency should grant Purchaser a non-exclusive, perpetual, fully paid-up license to use the pre-existing work in the form delivered to Purchaser as part of the service or deliverables for its internal business operations. Under such license, either of parties will have no right to sell the pre-existing work of the other party to a Third Party. Purchaser’s license to pre-existing work is conditioned upon its compliance with the terms of this Agreement and the perpetual license applies solely to the pre-existing work that bidder leaves with Purchaser at the conclusion of performance of the services.

4. **Residuals:**

In no event shall Implementation Agency be precluded from independently developing for itself, or for others, anything, whether in tangible or non-tangible form, which is competitive with, or similar to, the deliverables, set-out in this Agreement or Annexure. In addition, subject to the confidentiality obligations, Implementation Agency shall be free to use its general knowledge, skills and experience, and any ideas, concepts, know-how, and techniques that are acquired or used in the course of providing the Services.

5. **Right to monetize:**

   OIOS Application ownership rights vest solely with the Purchaser, including the right to monetize the complete product/deliverables supplied/developed by the Implementation Agency.

20. WARRANTY & MAINTENANCE

1. Standard:

The Implementation Agency warrants that the Project, including all the system(s), materials and goods supplied pursuant to the Agreement, shall be free from any defect or deficiency in the material, design, engineering, and workmanship that prevent the system and/or any of its systems(s) from fulfilling the technical requirements or that limit in a material fashion the performance, reliability, or extensibility of the system and/or any of its sub-system(s). Commercial warranty provisions of products supplied under the Agreement shall apply to the extent they do not conflict with the provisions of this Agreement.

a) The IA also warrants that the products, materials and other goods supplied under the Agreement are new, unused and incorporate all recent improvements in design that materially affect the system's or subsystem's ability to fulfil the technical requirements specified in the RFP.

b) In addition, the IA warrants that: (i) all Goods components to be incorporated into the System form part of the IA/OEM's and/or Subcontractor's current product lines.

c) The warranty period shall commence from the date of Go Live of the project or of any major component or subsystem for which phased Go-Live is provided for in the Agreement and shall extend for as follows:

Component	Period
Standard Hardware	6 months post completion of the agreement
COTS Software	6 months post completion of the agreement
Bespoke Software	6 months post completion of the agreement

Purchaser/Government department should approve signoff within 15 working days from the submission of deliverables for Go-Live/Phased Go-live (as relevant, depending on project requirement) by the implementing agency.

In case the Purchaser/Government department fails to respond and provide feedback on the above stated submission, the deliverables will be deemed accepted for the commencement of warranty for the project.

However, in case the purchaser confirms to vendor an alternative date, then the date would stand revised for deemed acceptance. Each deliverables shall be reviewed and approved at multiple levels. Duration of review required for each deliverable shall vary & the same would be finalized with the Implementation Agency at the project inception stage, following the principles laid down in section 5 & 6 of volume 1 of the RFP.

d) If during the warranty period any defect or deficiency is found in the material, design and performance/workmanship of the Project and other Services provided by the Implementation Agency, the Implementation Agency shall promptly, in consultation and agreement with Purchaser, and at the Implementation Agency's sole cost repair, replace, or otherwise make good (as the Implementation Agency shall, at its discretion, determine) such default, defect or deficiency as well as any damage to the system caused by such default, defect or deficiency. Any defective component, excluding hard disks, that has been replaced by the Implementation Agency shall remain the property of the Implementation Agency.

e) The IA may, with the consent of the Purchaser, remove from the site any product and other goods that are defective, if the nature of the defect, and/or any damage to the System caused by the defect, is such that repairs cannot be expeditiously carried out at the site. If the repair, replacement, or making good is of such a character that it may affect the efficiency of the System, the Purchaser may give the IA notice requiring that tests of the defective part be made by the IA immediately upon completion of such remedial work, whereupon the IA shall carry out such tests. If such part fails the tests, the IA shall carry out further repair, replacement, or making good (as the case may be) until that part of the System passes such tests. The tests shall be agreed upon by the Purchaser and the Supplier.

f) If the IA fails to commence the work necessary to remedy such defect or any damage to the System caused by such defect within a reasonable time period, the Purchaser may, following notice to the IA, proceed to do such work or contract a third party (or parties) to do such work, and the reasonable costs incurred by the Purchaser in connection with such work shall be paid to the Purchaser by the IA or may be deducted by the Purchaser from any amount due to the IA.

g) If the System or any of its sub-systems cannot be used by reason of such default, defect or deficiency and/or making good of such default, defect or deficiency, attributable to IA, the warranty period for the Project shall be extended by a period equal to the period during which the Project or any of its system could not be used by the Purchaser because of such defect and/or making good of such default, defect or deficiency. For reasons not attributable to IA, the IA shall not be liable.

h) Items substituted for defective parts of the System during the Warranty Period shall be covered by the Warranty for the remainder of the Warranty Period applicable for the part replaced or three (3) months, whichever is greater.

i) The Implementing Agency shall have no liability in the case of breach of this warranty due to (i) use of the deliverables on any environment (hardware or software) other than the environment recommended or approved by the Implementing Agency, (ii) the combination, operation, or use of some or all of the deliverables with information, software, specifications, instructions, data, or materials not recommended by the Implementing Agency; (iii) the deliverables having been tampered with, altered or modified by Purchaser without the written permission of the Implementing Agency, or (iv) use of the deliverables otherwise than in terms of the relevant documentation.

j) Implementation Agency will comply with all privacy and data protection laws, rules, and regulations that are in force or that may in the future be applicable. The Auditee and employees data of the purchaser shall never be used by the Implementation Agency (owner/partner/employees) or it's sub-contractor other than it's intended use.

2. **Implied Warranty:**

The warranties provided herein are in lieu of all other warranties, both express and implied, and all other warranties, including without limitation that of merchantability or fitness for intended purpose is specifically disclaimed.

21. LIQUIDATED DAMAGES

Time is the essence of the Agreement and the delivery dates are binding on the Implementation Agency. In the event of delay or any gross negligence in implementation of the project before Go-Live, for causes solely attributable to the Implementation Agency, in meeting the deliverables, the Purchaser shall be entitled at its option to recover from the Implementation Agency as agreed, liquidated damages, a sum of **0.5%** of the value of the deliverable which suffered delay or gross negligence for each completed week or part thereof subject to a limit of

10% of the total contract value. This right to claim any liquidated damages shall be without prejudice to other rights and remedies available to Purchaser under the contract and law.

22. INSURANCE COVER

1. Obligation to maintain insurance

In connection with the provision of the Services, the Service Provider must have and maintain:

a) for the Agreement Period, valid and enforceable insurance coverage for:

   i. public liability;

   ii. either professional indemnity or errors and omissions;

   iii. product liability;

   iv. workers' compensation as required by law; and

   v. any additional types specified in Schedule I; and

b) for 1 year following the expiry or termination of the Agreement, valid and enforceable insurance policies (if relevant), in the amount not less than the Insurance Cover specified in **ScheduleI**

2. Certificates of currency

The Implementation Agency must, on request by the Purchaser, provide current relevant confirmation of insurance documentation from its insurance brokers certifying that it has insurance as required by this Clause 23.The Service Provider agrees to replace any coverage prior to the date of expiry/cancellation.

3. Non-compliance

Purchaser or its nominated agencies may, at its election, terminate this Agreement as per clause 14, upon the failure of Implementation Agency or notification of such failure, to maintain the required insurance coverage. Inadequate insurance coverage for any reason shall not relieve Implementation Agency of its obligations under this Agreement.

23. MISCELLANEOUS

1. Personnel

a) The personnel assigned by Implementation Agency to perform the Services shall be employees of Implementation Agency, and under no circumstances shall such personnel be considered employees of Purchaser or its nominated agencies. The Implementation Agency shall have the sole responsibility for the supervision and control of the personnel deployed in the Project and for payment of such personnel's compensation, including salary, withholding of income taxes and social security taxes, worker's compensation, employee and disability benefits and the like and shall be responsible for all obligations of an employer subject to Applicable Law. Non employees to be employed only with prior written consent of the purchaser.

b) The Implementation Agency shall use its best efforts to ensure that sufficient Implementation Agency personnel are assigned to perform the Services and that such personnel have appropriate qualifications to perform the Services. After discussion with Implementation Agency, Purchaser or its nominated agencies shall have the right to require the removal or replacement of any Implementation Agency personnel performing work under this Agreement based on bonafide reasons. In the event that Purchaser or its nominated agencies requests that any Implementation Agency personnel be replaced, the substitution of such personnel shall be accomplished pursuant to a mutually agreed upon schedule.

c) In the event that the Purchaser and Implementation Agency identify any personnel of Implementation Agency as "Key Personnel", then the Implementation Agency shall not remove such personnel from the Project without the prior written consent of Purchaser or its nominated agencies unless such removal is the result of an unavoidable circumstance including but not limited to resignation, termination, medical leave, etc. The replacement of such key personnel shall be with prior written approval from the purchaser.

d) Except as stated in this Clause, nothing in this Agreement or the SLA will limit the ability of Implementation Agency to freely assign or reassign its employees; provided that Implementation Agency shall be responsible, at its expense, for transferring all appropriate knowledge from personnel being replaced to their replacements. Purchaser or its nominated agencies shall have the right to review and approve Implementation Agency's plan for any such knowledge transfer. Implementation Agency shall maintain the same or higher standards for skills and professionalism among replacement personnel as in personnel being replaced.

e) Each Party shall be responsible for the performance of all its obligations under this Agreement or the SLA as the case may be and shall be liable for the acts and omissions of its employees and agents in connection therewith.

f) Neither Party will solicit for employment or knowingly hire an employee of the other Party with whom such Party has contact pursuant to project engagements under this

Agreement. This restriction shall not apply to employees of either Party responding to advertisements in job fairs or news media circulated to the general public.

2. **Independent Contractor**

Nothing in this Agreement or the SLA shall be construed as establishing or implying any partnership or joint venture between the Parties to this Agreement or the SLA and, except as expressly stated in this Agreement or the SLA, nothing in this Agreement or the SLA shall be deemed to constitute any Parties as the agent of any other Party or authorizes either Party to:

a) incur any expenses on behalf of the other Party;
b) enter into any engagement or make any representation or warranty on behalf of the other Party;
c) pledge the credit of or otherwise bind or oblige the other Party; or
d) commit the other Party in any way whatsoever without in each case obtaining the other Party's prior written consent.

3. **Sub-contractors**

Implementation Agency shall only subcontract work related to (a) User Centralized Helpdesk and Training and Capacity Building to the extent indicated in Volume-I with Purchaser's prior written consent. No other work shall be sub contracted by the Implementation Agency. It is clarified that the Implementation Agency shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the sub-contractors. The Implementation Agency undertakes to indemnify the Purchaser or its nominated agencies from any claims on the grounds stated hereinabove.

4. **Assignment**

a) All terms and provisions of this Agreement shall be binding on and shall inure to the benefit of the Purchaser and their respective successors and permitted assigns.
b) Subject to Clause 5.1, the Implementation Agency shall not be permitted to assign its rights and obligations under this Agreement to any third party.
c) The Purchaser may assign or novate all or any part of this Agreement and Schedules/Annexures, and the Implementation Agency shall be a party to such novation, to any third party contracted to provide outsourced services to Purchaser or any of its nominees

5. Trademarks, Publicity

Neither Party may use the trademarks of the other Party without the prior written consent of the other Party except that Implementation Agency may, upon completion, use the Project as a reference for credential purpose. Except as required by law or the rules and regulations of each stock exchange upon which the securities of one of the Parties is listed, neither Party shall publish or permit to be published either along or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement, the SLA or the business of the Parties without prior reference to and approval in writing from the other Party, such approval not to be unreasonably withheld or delayed provided however that Implementation Agency may include Purchaser or its client lists for reference to third parties subject to the prior written consent of Purchaser not to be unreasonably withheld or delayed, Such approval shall apply to each specific case and relate only to that case.

6. Notices

a) Any notice or other document which may be given by either Party under this Agreement or under the SLA shall be given in writing in person or by pre-paid recorded delivery post, email or by facsimile transmission.

b) In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below:

<Insert Address> Tel:

Fax:

Email:

Contact:

With a copy to:

Implementation Agency

Tel:

Fax:

Email:

Contact:

In relation to a notice given under the MSA / SLA, a Party shall specify the Parties' address for service of notices, any such notice to be copied to the Parties at the addresses set out in this Clause.

a) Any such notice or other document shall be deemed to have been given to the other Party (or, if relevant, its relevant associated company) when delivered (if delivered in person) if delivered between the hours of 9.00 am and 5.00 pm at the address of the other Party set forth above or if sent by fax, provided the copy fax is accompanied by a confirmation of transmission, or on the next working day thereafter if delivered outside such hours, and 7 days from the date of posting (if by letter).
b) Either Party to this Agreement or to the SLA may change its address, telephone number, facsimile number and nominated contact for notification purposes by giving the other reasonable prior written notice of the new information and its effective date.

7. Variations and Further Assurance

a) No amendment, variation or other change to this Agreement or the SLA shall be valid unless authorised in accordance with the change control procedure as set out in the Change Control Schedule set out in Schedule I of this Agreement. Such amendment shall be made in written and signed by the duly authorised representatives of the Parties to this Agreement or the SLA.
b) Each Party to this Agreement or the SLA agrees to enter into or execute, without limitation, whatever other agreement, document, consent and waiver and to do all other things which shall or may be reasonably required to complete and deliver the obligations set out in this Agreement or the SLA

8. Severability and Waiver

a) If any provision of this Agreement or the SLA, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the SLA or the remainder of the provisions in question which shall remain in full force and effect. The relevant Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid or unenforceable provision a valid and enforceable provision which achieves to the greatest extent possible the economic, legal and commercial objectives of the illegal, invalid or unenforceable provision or part provision.
b) No failure to exercise or enforce and no delay in exercising or enforcing on the part of either Party to this Agreement or the SLA of any right, remedy or provision of this

Agreement or the SLA shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of such right, remedy or provision or the exercise or enforcement of any other right, remedy or provision.

9. **Compliance with Applicable Law**

Each Party to this Agreement accepts that its individual conduct shall (to the extent applicable to its business like the Implementation Agency as an information technology service provider) at all times comply with all laws, rules and regulations of government and other bodies having jurisdiction over the area in which the Services are undertaken provided that changes in such laws, rules and regulations which result in a change to the Services shall be dealt with in accordance with the Change Control Schedule set out in Schedule I of this Agreement.

10. **Professional Fees**

All expenses incurred by or on behalf of each Party to this Agreement and the SLA, including all fees of agents, legal advisors, accountants and actuaries employed by either of the Parties in connection with the negotiation, preparation and execution of this Agreement or the SLA shall be borne solely by the Party which incurred them.

11. **Ethics**

The Implementation Agency represents, warrants and covenants that it has given no commitments, payments, gifts, kickbacks, lavish or expensive entertainment, or other things of value to any employee or agent of Purchaser or its nominated agencies in connection with this agreement and acknowledges that the giving of any such payment, gifts, entertainment, or other things of value is strictly in violation of Purchaser standard policies and may result in cancellation of this Agreement, or the SLA.

12. **Entire Agreement**

This Agreement and the SLA with all schedules & annexures appended thereto and the contents and specifications of the RFP constitute the entire agreement between the Parties with respect to their subject matter, and as to all other representations, understandings or agreements which are not fully expressed herein, provided that nothing in this Clause shall be interpreted so as to exclude any liability in respect of fraudulent misrepresentation.

13. **Amendment**

Any amendment to this Agreement shall be made in accordance with the Change Control Schedule set out in Schedule I of this Agreement by mutual written consent of all the Parties.

24. GOVERNING LAW AND DISPUTE RESOLUTION

1. This Agreement shall be governed by and construed in accordance with the laws of India, without giving effect to conflict of law rules. The parties expressly agree to exclude the application of the U.N. Convention on Contracts for the International Sale of Goods (1980) to this Agreement and the performance of the parties contemplated under this Agreement, to the extent that such convention might otherwise be applicable.
2. Any dispute arising out of or in connection with this Agreement or the SLA shall in the first instance be dealt with in accordance with the escalation procedure as set out in the Governance Schedule set out as Schedule IV of this Agreement.
3. In case the escalations do not help in resolution of the problem within 3 weeks of escalation, both the parties should agree on a mediator for communication between the two parties. The process of the mediation would be as follows:
    - Aggrieved party should refer the dispute to the identified mediator in writing, with a copy tothe other party. Such a reference should contain a description of the nature of the dispute, the quantum in dispute (if any) and the relief or remedy sought suitable.
    - The mediator shall use his best endeavours to conclude the mediation within a certain numberof days of his appointment.
    - If no resolution can be reached through mutual discussion or mediation within 30 days thenthe matter should be referred to Experts for advising on the issue.
4. Any dispute or difference whatsoever arising between the parties to this Contract out of or relating to the construction, meaning, scope, operation or effect of this Contract or the validity of the breach thereof shall be referred to Delhi International Arbitration Center (established by the High Court of Delhi). The provisions of the Arbitration and Conciliation Act, 1996 will be applicable and the award made there under shall be final and binding upon the parties hereto, subject to legal remedies available under the law. Such differences shall be deemed to be a submission to arbitration under the Indian Arbitration and Conciliation Act, 1996, or of any modifications, Rules or re-enactments thereof. The Arbitration proceedings will be held at Delhi, India. Any legal dispute will come under the sole jurisdiction of Delhi, India.

5. Compliance with laws: Each party will comply with all applicable export and import laws and regulations.
6. Risk of Loss: For each hardware item, Implementation Agency bears the risk of loss or damage up to the time it is delivered to the Purchaser's designated location.
7. Third party components: Implementation Agency will provide all third party components solely on a pass-through basis in accordance with the relevant third party terms and conditions.

25. PERFORMANCE BANK GUARANTEE (PBG)

A Performance Bank Guarantee (PBG) of 10% of total contract value of the contract would be furnished by the implementation agency in the form of a Bank Guarantee as per the format provided in the RFP from any **Commercial Bank**. The PBG should be furnished within **15 days** from notification of award or on or before the date of signing the contract and should be valid till the entire term of the agreement and for an **additional period of 180 days** after the completion of term of agreement including warranty obligations.

In case any claims or any other contract obligations are outstanding, the Implementation Agency will extend the Performance Bank Guarantee as asked by the Purchaser till such time the Implementation Agency settles all claims and completes all contract obligations.

Notwithstanding what has been stated elsewhere in this Contract and the Schedules attached herein, in the event the Implementation Agency is unable to meet the obligations pursuant to the implementation of the Project and/or provide the operations and maintenance Services and any related scope of work as stated in this Contract, the Purchaser will, inter alia, have the option to invoke the Performance Bank Guarantee after serving a written notice fifteen days in advance on the Implementation Agency. Such right of the Implementation Agency shall be without prejudice to any other rights or remedies available under law or contract. In case the contract is extended, the PBG has to be valid for **180 days beyond the extended period**.

In the event of the expiry of this Agreement, IA&AD shall retain the Performance Bank Guarantee till it's validity period. Subsequently, the Performance Bank Guarantee shall be released provided

IA&AD or an agency nominated by IA&AD certifies and IA&AD accepts that the handing over procedure as stated in Exit Management Schedule has been duly complied with. In the event that the compliance is not completed, the Performance Bank Guarantee shall be invoked and the amount appropriated and forfeited. IA&AD will not pay any costs of Implementation Agency's conduct of business. There will be no payments to the Implementation Agency to compensate for business loss.

IN WITNESS WHEREOF the Parties have by duly authorized

Representatives set their respective hands and seal on the date first above Written in the presence of:

WITNESSES:

Signed by:

(Name and designation) **For and on behalf of Purchaser**

(FIRST PARTY)

Signed by:

(Name and designation)

IMPLEMENTATION AGENCY

(SECOND PARTY)

(Name and designation) For and on behalf of Implementation Agency Signed by:

26. SCHEDULES

SCHEDULE I – CHANGE CONTROL SCHEDULE

This Schedule describes the procedure to be followed in the event of any proposed change to the Master Service Agreement (“MSA”), Project Implementation Phase, SLA and Scope of Work and Functional Requirement Specifications. Such change shall include, but shall not be limited to, changes in the scope of services provided by the Implementation Agency and changes to the terms of payment as stated in the Terms of Payment Schedule.

The Purchaser and IA recognize that frequent change is an inevitable part of delivering services and that a significant element of this change can be accomplished by re-organizing processes and responsibilities without a material effect on the cost. The IA will endeavour, wherever reasonably practicable, to effect change without an increase in the terms of payment as stated in the Terms of Payment Schedule and Purchaser or its nominated agencies will work with the Implementation Agency to ensure that all changes are discussed and managed in a constructive manner. This Change Control Schedule sets out the provisions which will apply to all the changes to this agreement and other documents except for the changes in SLAs for which a separate process has been laid out in Clause 11 of the SLA.

This Change Control Schedule sets out the provisions which will apply to changes to the MSA.

CHANGE MANAGEMENT PROCESS

a. CHANGE CONTROL NOTE ("CCN")

i. Change requests in respect of the MSA, the Project Implementation, the operation, the SLA or Scope of work and Functional Requirement specifications will emanate from the Parties' respective Project Manager who will be responsible for obtaining approval for the change and who will act as its sponsor throughout the Change Control Process and will complete Part A of the CCN attached as Annexure A hereto. CCNs will be presented to the other Party's Project Manager who will acknowledge receipt by signature of the CCN.

ii. The IA and the Purchaser or its nominated agencies, during the Project Implementation Phase and the Purchaser or its nominated agencies during the Operations and Management Phase and while preparing the CCN, shall consider the change in the context of the following parameter, namely whether the change is beyond the scope of Services including ancillary and concomitant services required and as detailed in the RFP and is suggested and applicable only after the testing, commissioning and certification of the Pilot Phase and the Project Implementation Phases I & II as set out in this Agreement.

iii. It is hereby also clarified here that any change of control suggested beyond 25 % of the value of this Project will be beyond the scope of the change control process and will be considered as the subject matter for a separate bid process and a separate contract. It is hereby clarified that the 25% of the value of the Project as stated in herein above is calculated on the basis of project value submitted by the Implementation Agency and accepted by the Purchaser or its nominated agencies or as decided and approved by Purchaser or it Nominated Agencies. For arriving at the cost / rate for change upto 25% of the project value, the payment terms and relevant rates as specified in Annexure D shall apply.

b. Quotation

i. The IA shall assess the CCN and complete Part B of the CCN, in completing the Part B of the CCN the IA shall provide as a minimum:

1. a description of the change
2. a list of deliverables required for implementing thechange;
3. a time table for implementation;
4. an estimate of any proposed change
5. any relevant acceptance criteria
6. an assessment of the value of the proposed change;
7. material evidence to prove that the proposed change is not already covered within the Agreement and the scope of work

ii. Prior to submission of the completed CCN to the Purchaser, or its nominated agencies, the Service Provider will undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, the IA shall consider the materiality of the proposed change in the context of the MSA and the Project Implementation affected by the change and the total effect that may arise from implementation of the change.

c. Costs

Each Party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process provided the IA meets the obligations as set in the CCN. In case of recertification due to proposed changes, required cost will be borne by the party that initiated the change. In the event the IA is unable to meet the obligations as defined in the CCN, then the cost of getting it done by a third party will be borne by the IA.

d. Obligations

The IA shall be obliged to implement any proposed changes once approval in accordance with above provisions has been given, with effect from the date agreed for implementation and within an agreed timeframe. IA will not be obligated to work on a change until the parties agree in writing upon its scope, price and/or schedule impact. The cost associated with any hardware/goods/License for COTS product should not exceed the price quoted in the bidders proposal. Any costs associated with changes to Software specifications which cannot be arrived at on the basis of the IA's proposal shall be mutually agreed to between the IA and the Purchaser.

SCHEDULE II - EXIT MANAGEMENT SCHEDULE

1 PURPOSE

1.1 This Schedule sets out the provisions, which will apply on expiry or termination of the MSA, the Project Implementation, Operation and Management SLA.

1.2 In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.

1.3 The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

2 TRANSFER OF ASSETS

2.1 Purchaser shall be entitled to serve notice in writing on the IA at any time during the exit management period as detailed hereinabove requiring the IA and/or its sub-contractors to provide the Purchaser with a complete and up to date list of the Assets within 30 days of such notice. Purchaser shall then be entitled to serve notice in writing on the IA at any time prior to the date that is 30 days prior to the end of the exit management period requiring the IA to sell the Assets, if any, to be transferred to Purchaser or its nominated agencies at book value as determined as of the date of such notice in accordance with the provisions of relevant laws.

2.2 In case of contract being terminated by Purchaser, Purchaser reserves the right to ask IA to continue running the project operations for a period of 6 months after termination orders are issued.

2.3 Upon service of a notice under this Article the following provisions shall apply:

(i) in the event, if the Assets to be transferred are mortgaged to any financial institutions by the IA, the IA shall ensure that all such liens and liabilities have been cleared beyond doubt, prior to such transfer. All documents regarding the discharge of such lien and liabilities shall be furnished to the Purchaser.

(ii) All risk in and title to the Assets to be transferred / to be purchased by the Purchaser pursuant to this Article shall be transferred to Purchaser, on the last day of the exit management period.

(iii) Purchaser shall pay to the IA on the last day of the exit management period such sum representing the Net Block (procurement price less depreciation as per provisions of Companies Act) of the Assets to be transferred as stated in the Terms of Payment Schedule.

(iv) Payment to the outgoing IA shall be made to the tune of last set of completed services / deliverables, subject to SLA requirements.

(v) The outgoing IA will pass on to Purchaser and/or to the Replacement IA, the subsisting rights in any leased properties/ licensed products on terms not less favourable to Purchaser/ Replacement IA, than that enjoyed by the outgoing IA.

3 COOPERATION AND PROVISION OF INFORMATION

3.1 During the exit management period:

(i) The Implementation Agency will allow the Purchaser or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the Purchaser to assess the existing services being delivered;

(ii) promptly on reasonable request by the Purchaser, the IA shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by the Implementation Agency or subcontractors appointed by the Implementation Agency). The Purchaser shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The Implementation Agency shall permit the Purchaser or its nominated agencies to have reasonable access to its employees and facilities as reasonably required by Purchaser or Its Nominated agency, to understand the methods of delivery of the services employed by the Implementation Agency and to assist appropriate knowledge transfer.

4 CONFIDENTIAL INFORMATION, SECURITY AND DATA

4.1 The Implementation Agency will promptly on the commencement of the exit management period supply to the Purchaser or its nominated agency the following:

(i) information relating to the current services rendered and customer and performance data relating to the performance of subcontractors in relation to the services;

(ii) documentation relating to Computerization Project's Intellectual Property Rights;

(iii) documentation relating to sub-contractors;

(iv) all current and updated data as is reasonably required for purposes of Purchaser or its nominated agencies transitioning the services to its Replacement Implementation Agency in a readily available format nominated by the Purchaser, its nominated agency;

(v) all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable Purchaser or its nominated agencies, or its Replacement Implementation Agency to carry out due diligence in order to transition the provision of the Services to Purchaser or its nominated agencies, or its Replacement Implementation Agency (as the case may be).

4.2 Before the expiry of the exit management period, the Implementation Agency shall deliver to the Purchaser or its nominated agency all new or up-dated materials from the categories set out in the schedule above and shall not retain any copies thereof, except that the Implementation Agency shall be permitted to retain one copy of such materials for archival purposes only.

4.3 Before the expiry of the exit management period, unless otherwise provided under the MSA, the Purchaser or its nominated agency shall deliver to the Implementation Agency all forms of Implementation Agency confidential information.

5 EMPLOYEES

5.1 Promptly on reasonable request at any time during the exit management period, the Implementation Agency shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to the Purchaser or its nominated agency a list of all employees (with job titles) of the Implementation Agency dedicated to providing the services at the commencement of the exit management period.

5.2 Where any national, regional law or regulation relating to the mandatory or automatic transfer of the contracts of employment from the Implementation Agency to the Purchaser or its nominated agency, or a Replacement Implementation Agency ("***Transfer Regulation***") applies to any or all of the employees of the Implementation Agency, then the Parties shall comply with their respective obligations under such Transfer Regulations.

6 TRANSFER OF CERTAIN AGREEMENTS

On request by the Purchaser or its nominated agency the Implementation Agency shall effect such assignments, transfers, licences and sub-licences to the Product Owner or its Replacement Implementation Agency in relation to any equipment lease, maintenance or service provision agreement between Implementation Agency and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the Purchaser or its nominated agency or its Replacement Implementation Agency.

7 RIGHTS OF ACCESS TO PREMISES

7.1 At any time during the exit management period, where Assets are located at the Implementation Agency's premises, the Implementation Agency will be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) the Purchaser or its nominated agency and/or any Replacement Implementation Agency in order to make an inventory of the Assets.

7.2 The Implementation Agency shall also give the Purchaser or its nominated agency or its nominated agencies, or any Replacement Implementation Agency right of reasonable access to the Implementation Partner's premises and shall procure the Purchaser or its nominated agency or its nominated agencies and any Replacement Implementation Agency rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the MSA as is reasonably necessary to migrate the services to the Purchaser or its nominated agency, or a Replacement Implementation Agency.

8 GENERAL OBLIGATIONS OF THE IMPLEMENTATION AGENCY

8.1 The Implementation Agency shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the Purchaser or its nominated agency or its Replacement Implementation Agency and which the Implementation Agency has in its possession or control at any time during the exit management period.

8.2 For the purposes of this Schedule, anything in the possession or control of any Implementation Agency, associated entity, or sub-contractor is deemed to be in the possession or control of the Implementation Agency.

8.3 The Implementation Agency shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

9 EXIT MANAGEMENT PLAN

9.1 The Implementation Agency shall provide the Purchaser or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the MSA as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

(i) A detailed program of the transfer process that could be used in conjunction with a Replacement Implementation Agency including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;

(ii) plans for the communication with such of the Implementation Agency's subcontractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the Purchaser’s operations as a result of undertaking the transfer;

(iii) (if applicable) proposed arrangements for the segregation of the Implementation Agency's networks from the networks employed by Purchaser and identification of specific security tasks necessary at termination;

(iv) Plans for provision of contingent support to Purchaser, and Replacement Implementation Agency for a reasonable period after transfer.

9.2 The Implementation Agency shall re-draft the Exit Management Plan a s follows:

- Before OIOS application Phase 1 Go-live
- Before OIOS application Phase 2 Go-live
- Before OIOS application Phase 3 Go-live
- Annually for rest of the contract duration

9.3 Each Exit Management Plan shall be presented by the Implementation Agency for and approved by the Purchaser or its nominated agencies.

9.4 The terms of payment as stated in the Terms of Payment Schedule include the costs of the Implementation Agency complying with its obligations under this Schedule.

9.5 In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.

9.6 During the exit management period, the Implementation Agency shall use its best efforts to deliver the services.

9.7 Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

9.8 This Exit Management plan shall be furnished in writing to the Purchaser or its nominated agencies within 90 days from the Effective Date of this Agreement.

SCHEDULE III - AUDIT, ACCESS AND REPORTING

1 PURPOSE

This Schedule details the audit, access and reporting rights and obligations of the Purchaser or its nominated agency and the Implementation Agency.

1 AUDIT NOTICE AND TIMING

2.1 As soon as reasonably practicable after the Effective Date, the Parties shall use their best endeavours to agree to a timetable for routine audits during the Project Implementation Phase and the Operation and Management Phase. Such timetable during the Implementation Phase, the Purchaser or its nominated agency and thereafter during the operation Phase, the Purchaser or its nominated agency shall conduct routine audits in accordance with such agreed timetable and shall not be required to give the Implementation Agency any further notice of carrying out such audits.

2.2 The Purchaser or its nominated agency may conduct non-timetabled audits at his/ her own discretion if it reasonably believes that such non-timetabled audits are necessary as a result of an act of fraud by the Implementation Agency, a security violation, or breach of confidentiality obligations by the Implementation Agency, provided that the requirement for such an audit is notified in writing to the Implementation Agency a reasonable period time prior to the audit (taking into account the circumstances giving rise to the reasonable belief) stating in a reasonable level of detail the reasons for the requirement and the alleged facts on which the requirement is based. If the Implementation Agency considers that the non-timetabled audit was not appropriate, the matter shall be referred to the escalation procedure as set out in the Governance Schedule.

2.3 The frequency of audits shall maximum half yearly, provided always that the Purchaser or its nominated agency shall endeavour to conduct such audits with the lowest levels of inconvenience and disturbance practicable being caused to the Implementation Agency. Any such audit shall be conducted by with adequate notice of 2 weeks to the Implementation Agency.

2.4 Purchaser will ensure that any 3rd party agencies appointed to conduct the audit will not be competitor of the Implementation Agency and will be bound by confidentiality obligations.

2 ACCESS

The Implementation Agency shall provide to the Purchaser or its nominated agency reasonable access to employees, subcontractors, suppliers, agents and third party facilities as detailed in the RFP, documents, records and systems reasonably required for audit and shall provide all such persons with routine assistance in connection with the audits and inspections. The Product Owner shall have the right to copy and retain copies of any relevant records. The Implementation Agency shall make every reasonable effort to co-operate with them.

3 AUDIT RIGHTS

4.1 The Purchaser or its nominated agency shall have the right to audit and inspect suppliers, agents and third party facilities (as detailed in the RFP), documents, records, procedures and systems relating to the provision of the services, but only to the extent that they relate to the provision of the services, as shall be reasonably necessary to verify:

(i) The security, integrity and availability of all data processed, held or conveyed by the Partner on behalf of Purchaser and documentation related thereto;

(ii) That the actual level of performance of the services is the same as specified in the SLA;

(iii) That the Implementation Agency has complied with the relevant technical standards, and has adequate internal controls in place; and

(iv) The compliance of the Implementation Agency with any other obligation under the MSA and SLA.

(v) Security audit and implementation audit of the system shall be done once each year, the cost of which shall be borne by the Implementation Agency.

(vi) For the avoidance of doubt the audit rights under this Schedule shall not include access to the Implementation Agency's profit margins or overheads, any confidential information relating to the Implementation Agency’ employees, or (iii) minutes of its internal Board or Board committee meetings including internal audit, or (iv) such other information of commercial-in-confidence nature which are not relevant to the Services associated with any obligation under the MSA.

4 AUDIT RIGHTS OF SUB-CONTRACTORS, SUPPLIERS AND AGENTS

4.2 The Implementation Agency shall use reasonable endeavours to ensure the same audit and access provisions as defined in this Schedule with sub-contractors who supply labour, services in respect of the services. The Implementation Agency shall inform the Purchaser or its nominated agency prior to concluding any sub-contract or supply agreement of any failure to achieve the same rights of audit or access.

4.3 REPORTING: The Implementation Agency will provide quarterly reports to the Product Owner or Officer designated by him/her, regarding any specific aspects of the Project and in context of the audit and access information as required by the Purchaser or its nominated agency.

5 ACTION AND REVIEW

5.1 Any change or amendment to the systems and procedures of the Implementation Agency, or sub- contractors, where applicable arising from the audit report shall be agreed within thirty (30) calendar days from the submission of the said report.

5.2 Any discrepancies identified by any audit pursuant to this Schedule shall be immediately notified to the Purchaser or its nominated agency and the Implementation Agency Project Manager who shall determine what action should be taken in respect of such discrepancies in accordance with the terms of the MSA.

6 TERMS OF PAYMENT

The Purchaser shall bear the cost of any audits and inspections. The terms of payment are exclusive of any costs of the Implementation Agency and the sub-contractor, for all reasonable assistance and information provided under the MSA, the Project Implementation, Operation and Management SLA by the Implementation Agency pursuant to this Schedule.

7 RECORDS AND INFORMATION

For the purposes of audit in accordance with this Schedule, the Implementation Agency shall maintain true and accurate records in connection with the provision of the services and the Implementation Agency shall handover all the relevant records and documents upon the termination or expiry of the MSA.

SCHEDULE IV - GOVERNANCE SCHEDULE

Refer section 6 of volume 1

SCHEDULE V - TERMS OF PAYMENT SCHEDULE

Refer section 8 of Volume 2

27. ANNEXURE

ANNEXURE A – FORMAT FOR CHANGE CONTROL NOTICE

Change Control Note	**CCN Number:**
Part A: Initiation	
Title:	
Originator:	
Sponsor:	
Date of Initiation:	
Details of Proposed Change	
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Authorised by Purchaser	Date:
Name:	
Signature: Received by the IA	Date:
Name:	
Signature:	
Change Control Note	**CCN Number:**
Part B : Evaluation	
(Identify any attachments as B1, B2, and B3 etc.) Changes to Services, charging structure, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.	

Brief Description of Solution:	
Impact:	
Deliverables:	
Timetable:	
Charges for Implementation: (including a schedule of payments)	
Other Relevant Information: (including value-added and acceptance criteria)	
Authorised by the Implementation Agency	**Date:**
Name:	
Signature:	

Change Control Note	**CCN Number :**
Part C : Authority to Proceed	
Implementation of this CCN as submitted in Part A, in accordance with Part B is: (tick as appropriate)	
Approved	

Rejected **Requires Further Information** (as follows, or as Attachment 1 etc.)	
For Purchaser and its nominated agencies	**For the Implementation Agency**
Signature	Signature
Name	Name
Title	Title
Date	Date

ANNEXURE B - LIST OF SERVICES PROVIDED BY THE IMPLEMENTATION AGENCY

Various services to be offered by the Implementation Agency will consist of:

i.

ii.

iii.

iv.

v.

Note:

➢ Purchaser will sign the end user license agreement for the software brought from any 3rd party for the purpose of this Project however Implementation Agency shall be solely responsible to make payment for the cost of software to such third party software vendor.

ANNEXURE C –REQUIRED DELIVERABLE AND ASSOCIATED TIMELINES

Refer section 8 of volume 2

ANNEXURE D – BID

1. TECHNICAL BID RESPONSE – EXTRACTED AS APPENDIX – A
2. FINANCIAL BID RESPONSE

   2a. Summary of Cost Components

   2b. Summary of Man-month rates
3. Details of Cost Component

ANNEXURE E – BILL OF MATERIAL

ANNEXURE F – ROLES AND RESPONSIBILITIES OF THE PARTIES

<to be inserted later>

28. NON-DISCLOSURE AGREEMENT

THIS AGREEMENT is made on this the <***> day of <***> 20--- at <***>, India.

BETWEEN

-- having its office at --- India hereinafter referred to as **'*Purchaser*'** or **'-----------------',** which expression shall, unless the context otherwise requires, include its permitted successors and assigns);

AND

<***>**,** a Company incorporated under the *Companies Act, 1956* or Companies Act, 2013 or limited liability partnership (LLP) under LLP Act, 2008 , having its registered office at <***> (hereinafter referred to as '***the Implementation Agency/IA'*** which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as the '***Parties***' and individually as a '***Party***'.

WHEREAS:

1. Purchaser is desirous to implement the project of ------------------------------ --.
2. The Purchaser and Implementation Agency have entered into a Master Services Agreement dated <***> (the "***MSA***") as well as a Service Level Agreement dated <***> (the "***SLA***") in furtherance of the Project.
3. Whereas in pursuing the Project (the "***Business Purpose***"), a Party ("Disclosing Party) recognizes that they will disclose certain Confidential Information (*as defined hereinafter*) to the other Party ("Receiving Party").
4. Whereas such Confidential Information (*as defined hereinafter*) belongs to Receiving Party as the case may be and is being transferred to the Disclosing Party to be used only for the Business Purpose and hence there is a need to protect such information from unauthorized use and disclosure.

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

Terms and expressions used in this Agreement (including the Introduction) shall have the same meanings set out in Clause I of MSA.

1.2 Interpretation

In this Agreement, unless otherwise specified:

(a) references to Clauses, Sub-Clauses, Paragraphs and Schedules are to clauses, sub-clauses, paragraphs of and schedules to this Agreement;

(b) use of any gender includes the other genders;

(c) references to a '**company**' shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established;

(d) references to a '**person**' shall be construed so as to include any individual, firm, company, government, state or agency of a state, local or municipal authority or government body or any joint venture, association or partnership (whether or not having separate legal personality);

(e) a reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re- enacted;

(f) any reference to a '**day**' (including within the phrase 'business day') shall mean a period of 24 hours running from midnight to midnight;

(g) references to a **'business day'** shall be construed as a reference to a day (other than a Sunday) on which banks in the state of Delhi are generally open for business;

(h) references to times are to Indian standard time;

(i) a reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and

(j) all headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

1.3 Measurements and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to 2 (two) decimal places, with the third digit of 5 (five) or above being rounded up and below 5 (five) being rounded down except in money calculations where such amounts shall be rounded off to the nearest INR.

1.4 Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

(a) as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;

(b) as between the provisions of this Agreement and the Schedules, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules; and

(c) as between any value written in numerals and that in words, the value in words shall prevail.

1.5 Priority of agreements

The Parties hereby expressly agree that for the purpose of giving full and proper effect to this Agreement, the MSA and this Agreement shall be read together and construed harmoniously. In the event of any conflict between the MSA and this Agreement, the provisions contained in the MSA shall prevail over this Agreement.

2. TERM

This Agreement will remain in effect for five years from the date of the last disclosure of Confidential Information ("***Term***"), at which time it will terminate, unless extended by the disclosing party in writing.

3. SCOPE OF THE AGREEMENT

(a) This Agreement shall apply to all confidential and proprietary information disclosed by Disclosing Party to the Receiving Party and other information which the disclosing party identifies in writing or otherwise as confidential before or within (30) thirty days after disclosure to the Receiving Party ("Confidential Information"). Such Confidential Information consists of certain specifications, documents, software, prototypes and/or technical information, and all copies and derivatives containing such Information that may be disclosed to the Disclosing Party for and during the Business Purpose, which a party considers proprietary or confidential.

(b) Such Confidential Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, or through visual observation or by any other means to the Receiving Party.

4. OBLIGATIONS OF THE RECEIVING PARTY

The Receiving Party shall:

(a) Use the Confidential Information only for the Business Purpose and shall hold the Confidential Information in confidence using the same degree of care as it normally exercises to protect its own proprietary information, taking into account the nature of the Confidential Information, and

(b) Grant access to Confidential Information only to its employees on a 'need to know basis' and restrict such access as and when not necessary to carry out the Business Purpose.

(c) Cause its employees to comply with the provisions of this Agreement;

(d) Reproduce Confidential Information only to the extent essential to fulfilling the Business Purpose, and

(e) Prevent disclosure of Confidential Information to third parties;

(f) Disclose the Confidential Information to its consultants/contractors on a need to know basis; provided that by doing so, the Receiving Party agrees to bind such consultants/ contractors to terms at least as restrictive as those stated herein. The Receiving Party upon making a disclosure under this Clause shall:

    i. Advise the consultants/contractors of the confidentiality obligations imposed on them by this Clause.

(g) Upon the Disclosing Party's request, the Receiving Party shall either return to the disclosing party all Confidential Information or shall certify to the disclosing party that all media containing Confidential Information have been destroyed. Provided, however, that an archival copy of the Confidential Information may be retained in the files of the Receiving Party's counsel, solely for the purpose of proving the contents of the Confidential Information.

(h) Not to remove any of the other Party's Confidential Information from the premises of the Disclosing Party without prior written approval.

(i) Exercise extreme care in protecting the confidentiality of any Confidential Information which is removed, only with the Disclosing Party's prior written approval, from the Disclosing Party's premises. Each Party agrees to comply with any and all terms and conditions the disclosing party may impose upon any such approved removal, such as conditions that the removed Confidential Information and all copies must be returned by a certain date, and that no copies are to be made off of the premises.

(j) Upon the Disclosing Party’s request, the Receiving Party shall promptly return to the Disclosing Party all tangible items containing or consisting of the disclosing party’s Confidential Information all copies thereof.

5. EXCEPTIONS TO CONFIDENTIAL INFORMATION

The foregoing restrictions on each party's use or disclosure of Confidential Information shall not apply to the Confidential Information that the Receiving Party can demonstrate that such Confidential Information:

(a) was independently developed by or for the Receiving Party without reference to the Information, or was received without restrictions; or

(b) has become generally available to the public without breach of confidentiality obligations of the Receiving Party; or

(c) was in the Receiving Party's possession without restriction or was known by the Receiving Party without restriction at the time of disclosure; or

(d) is the subject of a subpoena or other legal or administrative demand for disclosure; provided, however, that the Receiving Party has given the disclosing party prompt notice of such demand for disclosure and the Receiving Party reasonably cooperates with the disclosing party's efforts to secure an appropriate protective order; or

(e) is disclosed with the prior consent of the disclosing party; or

(f) was in its possession or known to it by being in its use or being recorded in its files or computers or other recording media prior to receipt from the disclosing party and was not previously acquired by the Receiving Party from the disclosing party under an obligation of confidence; or

(g) the Receiving Party obtains or has available from a source other than the disclosing party without breach by the Receiving Party or such source of any obligation of confidentiality or non-use towards the disclosing party.

6. OWNERSHIP OF THE CONFIDENTIAL INFORMATION

(a) Each Party recognizes and agrees that all of the disclosing Party’s Confidential Information is owned solely by the Disclosing Party (or its licensors) and that the unauthorized disclosure or use of such Confidential Information would cause irreparable harm and significant injury, the degree of which may be difficult to ascertain.

(b) By disclosing the Confidential Information or executing this Agreement, Disclosing Party does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right. The Disclosing Party disclaims all warranties regarding the information, including all warranties with respect to infringement of intellectual property rights and all warranties as to the accuracy or utility of such information.

(c) Access to Confidential Information hereunder shall not preclude an individual who has seen such Confidential Information for the purposes of this Agreement from working on future projects for the Disclosing Party which relate to similar subject matters, provided that such individual does not make reference to the Confidential Information and does not copy the substance of the Confidential Information during the Term. Furthermore, nothing contained herein shall be construed as imposing any restriction on the Receiving Party's disclosure or use of any general learning, skills or know-how developed by the Receiving Party's personnel under this Agreement.

(d) Execution of this Agreement and the disclosure of Confidential Information pursuant to this Agreement do not constitute or imply any commitment, promise, or inducement by either Party to make any purchase or sale, or to enter into any additional agreement of any kind.

7. DISPUTE RESOLUTION

(a) If a dispute arises in relation to the conduct of this Contract (Dispute), a party must comply with this clause 7 before starting arbitration or court proceedings (except proceedings for urgent interlocutory relief). After a party has sought or obtained any urgent interlocutory relief that party must follow this clause 7.

(b) A party claiming a Dispute has arisen must give the other parties to the Dispute notice setting out details of the Dispute.

(c) During the 14 days after a notice is given under clause 7(b) (or longer period if the parties to the Dispute agree in writing), each party to the Dispute must use its reasonable efforts through a meeting of Senior Executive (or their nominees) to resolve the Dispute. If the parties cannot resolve the Dispute within that period then any such dispute or difference whatsoever arising between the parties to this Contract out of or relating to the construction, meaning, scope, operation or effect of this Contract or the validity of the breach thereof shall be referred to a sole arbitrator to be appointed by mutual consent of both the parties herein. If the parties cannot agree on the appointment of the arbitrator within a period of one month from the notification by one party to the other of existence of such dispute, then it shall be referred to Delhi International Arbitration Center (established by the High Court of Delhi). The provisions of the Arbitration and Conciliation Act, 1996 will be applicable and the award made there under shall be final and binding upon the parties hereto, subject to legal remedies available under the law. Such differences shall be deemed to be a submission to arbitration under the Indian Arbitration and Conciliation Act, 1996, or of any modifications, Rules or re-enactments thereof. The Arbitration proceedings will be held at the jurisdiction specified in Item 27. Any legal dispute will come under the sole jurisdiction specified in Item 27.

(d) The Receiving Party agrees that the Disclosing Party shall have the right to obtain an immediate injunction enjoining any breach of this Agreement, as well as the right to pursue any and all other rights and remedies available at law or in equity for such a breach.

8. VARIATION

This Agreement may only be varied in writing and signed by both Parties.

9. WAIVER

Waiver including partial or conditional waiver, by either Party of any default by the other Party in the observance and performance of any provision of or obligations under this Agreement:-

(a) shall be in writing

(b) shall not operate or be construed as a waiver of any other or subsequent default hereof or of other provisions of or obligations under this Agreement;

(c) shall be executed by a duly authorized representative of the Party; and

(d) shall not affect the validity or enforceability of this Agreement in any manner.

10. EXCLUSION OF IMPLIED WARRANTIES

This Agreement expressly excludes any warranty, condition or other undertaking implied at law or by custom or otherwise arising out of any other agreement between the Parties or any representation by either Party not contained in a binding legal agreement executed by both Parties.

11. ENTIRE AGREEMENT

This Agreement and the Annexure together constitute a complete and exclusive statement of the terms of the agreement between the Parties on the subject hereof, and no amendment or modification hereto shall be valid and effective unless such modification or amendment is agreed to in writing by the Parties and duly executed by persons especially empowered in this behalf by the respective Parties. All prior written or oral understandings, offers or other communications of every kind pertaining to this Agreement are abrogated and withdrawn.

12. SEVERABILITY

If for any reason whatever, any provision of this Agreement is or becomes invalid, illegal or unenforceable or is declared by any court of competent jurisdiction or any other instrumentality to be invalid, illegal or unenforceable, the validity, legality or enforceability of the remaining provisions shall not be affected in any manner, and the

Parties shall negotiate in good faith with a view to agreeing to one or more provisions which may be substituted for such invalid, unenforceable or illegal provisions, as nearly as is practicable to such invalid, illegal or unenforceable provision. Failure to agree upon any such provisions shall not be subject to the dispute resolution procedure set forth under this Agreement or otherwise.

13. NO PARTNERSHIP

This Agreement shall not be interpreted or construed to create an association, joint venture or partnership between the Parties, or to impose any partnership obligation or liability upon either Party, and neither Party shall have any right, power or authority to enter into any agreement or undertaking for, or act on behalf of, or to act as or be an agent or representative of, or to otherwise bind, the other Party except as expressly provided under the terms of this Agreement.

14. THIRD PARTIES

This Agreement is intended solely for the benefit of the Parties and their respective successors and permitted assigns, and nothing in this Agreement shall be construed to create any duty to, standard of care with reference to, or any liability to, any person not a Party to this Agreement.

15. SUCCESSORS AND ASSIGNS

The Agreement shall be binding on and shall inure to the benefit of the Parties and their respective successors and permitted assigns.

16. NOTICES

Any notice or other communication to be given by any Party to the other Party under or in connection with the matters contemplated by this Agreement shall be in writing and shall be given by hand delivery, recognized courier, registered post, email or facsimile transmission and delivered or transmitted to the Parties at their respective addresses set forth below:

If to Purchaser:

Attn: <***>

Tel:

Fax:

Email:

Contact:

With a copy to:

If to the Implementation Agency:

Attn. <***>

Phone: <***>

Fax No. <***>

17. LANGUAGE

All notices required to be given by one Party to the other Party and all other communications, documentation and proceedings which are in any way relevant to this Agreement shall be in writing and in the English language.

18. COUNTERPARTS

This Agreement may be executed in counterparts, each of which, when executed and delivered, shall constitute an original of this Agreement.

19. MITIGATION

Without prejudice to any express provisions of this Agreement on any mitigation obligations of the Parties, each of the Purchaser and the Implementation Agency shall at all times take all reasonable steps to minimize and mitigate any loss for which the relevant Party is entitled to bring a claim against the other Party pursuant to this Agreement.

20. REMOVAL OF DIFFICULTIES

The Parties acknowledge that it is conceivable that the Parties may encounter difficulties or problems in the course of implementation of the Project and the transactions envisaged under this Agreement. The Parties agree and covenant that they shall mutually discuss such difficulties and problems in good faith and take all reasonable steps necessary for removal or resolution of such difficulties or problems.

IN WITNESS WHEREOF THE PARTIES HAVE EXECUTED ANDDELIVERED THIS AGREEMENT AS OF THE DATE FIRST ABOVE WRITTEN.

SIGNED, SEALED AND DELIVERED	SIGNED, SEALED AND DELIVERED
For and on behalf of the Implementation Agency by:	For and on behalf of the Purchaser

(Signature)	(Signature)
(Name)	(Name)
(Designation)	(Designation)
(Address)	(Address)
(Fax No.)	(Fax No.)

In the presence of:

1.

2.

29. SERVICE LEVEL AGREEMENT

THIS AGREEMENT is made on this the <***> day of <***> 20--- at <***>, India.

BETWEEN

--- having its office at ------------------- --- India hereinafter referred to as ***'Purchaser'*** or **'------------ -----',** which expression shall, unless the context otherwise requires, include its permitted successors and assigns);

AND

<***>**,** a Company incorporated under the *Companies Act, 1956* or Companies Act, 2013 or limited liability partnership (LLP) under LLP Act, 2008, having its registered office at <***> (hereinafter referred to as '***the Implementation Agency/IA'*** which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as the '***Parties***' and individually as a '***Party***'.

WHEREAS:

1. Purchaser is desirous to implement the project of ----------------------------- --.
2. The Purchaser and Implementation Agency have entered into a Master Services Agreement dated <***> (the "***MSA***") as well as a Service Level Agreement dated <***> (the "***SLA***") in furtherance of the Project.

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

1. DEFINITIONS AND INTERPRETATION

a) Definitions

Terms and expressions used in this Agreement (including the Introduction) shall have the meanings set out in Annexure A.

b) Interpretation

In this Agreement, unless otherwise specified:

a) references to Clauses, Sub-Clauses, Paragraphs and Schedules are to clauses, sub-clauses, paragraphs of and schedules to this Agreement;

b) use of any gender includes the other genders;

c) references to a ‘company’ shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established;

d) references to a ‘person’ shall be construed so as to include any individual, firm, company, government, state or agency of a state, local or municipal authority or government body or any joint venture, association or partnership (whether or not having separate legal personality);

e) a reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted;

f) any reference to a ‘day’ (including within the phrase ‘business day’) shall mean a period of 24 hours running from midnight to midnight;

g) references to a ‘business day’ shall be construed as a reference to a day (other than a Sunday) on which banks in the state of Delhi are generally open for business;

h) references to times are to Indian Standard Time;

i) a reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and

j) all headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

c) Measurements and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to 2 (two) decimal places, with the third digit of 5 (five) or above being rounded up and below 5 (five) being rounded down except in money calculations where such amounts shall be rounded off to the nearest INR.

d) Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

a) as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;

b) as between the provisions of this Agreement and the Schedules, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules; and

c) as between any value written in numerals and that in words, the value in words shall prevail.

e) Priority of agreements

The Parties hereby expressly agree that for the purpose of giving full and proper effect to this Agreement, the MSA and this Agreement shall be read together and construed harmoniously. In the event of any conflict between the MSA and this Agreement, the provisions contained in the MSA shall prevail over this Agreement.

2. STRUCTURE

This SLA shall operate as a legally binding services agreement specifying terms which apply to the Parties in relation to the provision of the Services by the Implementation Agency to the Purchaser and its nominated agencies under this Agreement and the MSA.

3. OBJECTIVES OF THIS SLA

The Implementation Agency shall be required to ensure that the Service Levels which shall ensure the vision laid down in para 4.3 of volume 1 of the RFP.

To meet the aforementioned objectives the Implementation Agency will provide the Service Levels in accordance with the performance metrics as set out in detail in this Agreement. Further this Agreement shall govern the provision of the contracted services of the Implementation Agency to the Purchaser and its nominated agencies after the Go-Live Date.

4. SCOPE OF SLA

This Agreement has been executed in relation to the outsourcing portion of the Project between the Parties. The detailed Service Levels have been set out in Annexure A to this Agreement.

This Agreement shall ensure the following:

a) Establishment of mutual responsibilities and accountability of the Parties;
b) Definition each Party’s expectations in terms of services provided;
c) Establishment of the relevant performance measurement criteria;
d) Definition of the availability expectations;
e) Definition of the escalation process;
f) Establishment of trouble reporting single point of contact; and
g) Establishment of the framework for SLA change management

The following parties are obligated to follow the procedures as specified by this Agreement:

a) Purchaser

b) Implementation Agency

5. AGREEMENT OWNERS

The following personnel shall be notified to discuss the Agreement and take into consideration any proposed SLA change requests:

Name	Title	Telephone	Email
Purchaser	Authorized Representative, Purchaser	<***>	<***>
Implementation Agency	<***>	<***>	<***>

6. CONTACT LIST

In the event that there is any change in the listed contacts, the same shall be communicated and updated prior to such change occurring. The Single Point of Contact ("POC") for the Implementation Agency shall be <***> and will be available 24X7.

Name	Title	Location	Telephone
Purchaser	Authorized Representative, Purchaser	<***>	<***>
Implementation Agency	<***>	<***>	<***>

7. PRINCIPAL CONTACTS

The Purchaser and the Implementation Agency will nominate a senior staff member to be the principal contact regarding operation of this Agreement. At the date of signing of this Agreement, the nominated principal contacts are:

Buyer principal contact: ___________________________

Implementation Agency principal contact: _________________________

8. COMMENCEMENT AND DURATION OF THIS AGREEMENT

Agreement shall commence on the date of signing the contract (hereinafter the “SLA Effective Date”) and shall, unless terminated earlier in accordance with its terms or unless otherwise agreed by the Parties, expire on the date on which this Agreement expires or terminates, which shall be a period of **7** years starting from **<Go-live date>.**

9. EXCLUSIONS TO THE AGREEMENT

This Agreement shall not govern the following services:

a) Consulting services; and
b) Implementation Agency’s business processes not related to the Project.

10. TERMS OF PAYMENT AND PENALTIES

a) In consideration of the Services and subject to the provisions of the MSA and this Agreement, the Purchaser shall pay the amounts in accordance with the Terms of Payment Schedule of the MSA.
b) For the avoidance of doubt, it is expressly clarified that the Purchaser and/or its nominated agencies may also calculate a financial sum and debit the same against the terms of payment as defined in the Terms of Payment Schedule of the MSA as a result of the failure of the Implementation Agency to meet the Service Levels as set out in Annexure A of this Agreement, such sum being determined in accordance with the terms of the Service as set out in Annexure A of this Agreement.

11. UPDATING OF THIS AGREEMENT

a) The Parties anticipate that this Agreement shall need to be re-evaluated and modified to account for changes in work environment and technology from time to time. Hence they herby agree to revise the terms of the Agreement on an annual basis.
b) The Parties hereby agree upon the following procedure for revising this Agreement:
   i. Any and all changes to this Agreement will be initiated in writing between the Purchaser and the Implementation Agency, The service levels in this Agreement shall be considered to be standard for the Purchaser and shall only be modified if both Parties agree to an appended set of terms and conditions;
   ii. Only the Purchaser or the Implementation Agency may initiate a revision to this Agreement;
   iii. A notice of the proposed revision (“**SLA Change Request**”) shall be served to the Purchaser or the Implementation Agency as the case may be;

iv. The SLA Change request would be deemed to be denied in case it is not approved within a period of <***> days;

v. In the event that Buyer/Implementation Agency approves of the suggested change the change shall be communicated to all the Parties and the SLA Change request would be appended to the Agreement;

vi. The Purchaser shall update and republish the text of Agreement annually to include all the SLA Change Requests that have been appended to the Agreement during the course of the year. Such republished Agreement shall be circulated to all the Parties within <***> days of such change taking place.

12. DOCUMENT HISTORY

All revisions made to this Agreement shall be listed in chronological order as per the format set out below and a copy of the same shall be provided to the Parties:

Version	Date	Description of Change
<*>**	<***>	<***>
<*>**	<***>	<***>

13. SCOPE OF SERVICES

a) The Implementation Agency shall ensure that Services are available at various locations as per the requirements of the project;

b) The Implementation Agency shall provide support services for addressing problems related to the provision of services of the selected bidder through the POC. Such POC shall be available over telephone on <***> number 24 hours a day, 7 days a week

c) The Implementation Agency guarantees that he shall achieve the Service Levels for the Project;

d) The Implementation Agency shall be liable to Service Credits in case of failure to comply with the Service Levels. However any delay not attributable to the Implementation Agency shall not be taken into account while computing adherence to the Service Levels.

14. PERFORMANCE REVIEW

The POC's of both the Purchaser and the Implementation Agency shall meet on a quarterly basis to discuss priorities, service levels and system performance. Additional meetings may be held at the request of either the Implementation Agency or the Buyer. The agenda for these meetings shall be as follows:

a) Service performance;
b) Review of specific problems/exceptions and priorities; and
c) Review of the operation of this Agreement and determine corrective action to overcome deficiencies.

15. REPRESENTATIONS AND WARRANTIES OF BUYER

The Purchaser hereby represents and warrants to the Implementation Agency as follows:

a) it has full power and authority to execute, deliver and perform its obligations under this Agreement and to carry out the transactions contemplated herein and that it has taken all actions necessary to execute this Agreement, exercise its rights and perform its obligations, under this Agreement and carry out the transactions contemplated hereby;
b) it has taken all necessary actions under Applicable Law to authorize the execution, delivery and performance of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;
c) it has the financial standing and capacity to perform its obligations under the Agreement;
d) this Agreement has been duly executed by it and constitutes a legal, valid and binding obligation enforceable against it in accordance with the terms hereof and its obligations under this Agreement shall be legally valid, binding and enforceable obligations against it in accordance with the terms thereof;
e) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default under, or accelerate performance required by any of the Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;
f) there are no actions, suits or proceedings pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the default or breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform its material (including any payment) obligations under this Agreement;
g) it has no knowledge of any violation or default with respect to any order, writ, injunction or any decree of any court or any legally binding order of any Government Instrumentality which may result in any material adverse effect on the Implementation Agency's ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement.

16. REPRESENTATIONS AND WARRANTIES OF THE IMPLEMENTATION AGENCY

The Implementation Agency hereby represents and warrants to the Purchaser as follows:

a) it is duly organized and validly existing under the laws of India, and has full power and authority to execute and perform its obligations under this Agreement and to carry out the transactions contemplated hereby;

b) it has taken all necessary corporate and other actions under Applicable Laws to authorize the execution and delivery of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;

c) this Agreement has been duly executed by it and constitutes its legal, valid and binding obligation, enforceable against it in accordance with the terms hereof, and its obligations under this Agreement shall be legally valid, binding and enforceable obligations against it in accordance with the terms hereof;

d) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default under, or accelerate performance required by any of the terms of its Memorandum and Articles of Association or any Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

e) there are no actions, suits, proceedings, or investigations pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform any of its material obligations under this Agreement;

f) it has no knowledge of any violation or default with respect to any order, writ, injunction or decree of any court or any legally binding order of any government instrumentality which may result in any material adverse effect on its ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement;

g) it has complied with Applicable Law in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may have a material adverse effect on its ability to perform its obligations under this Agreement;

h) no representation or warranty by it contained herein or in any other document furnished by it to the Purchaser or to any government instrumentality in relation to the Required Consents contains or shall contain any untrue or misleading statement of material fact or omits or shall omit to state a material fact necessary to make such representation or warranty not misleading; and

i) no sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for entering into this Agreement or for influencing or attempting to influence any officer or employee of the Purchaser in connection therewith.

17. INDEMNITIES

The Parties agree to indemnify each other under this Agreement in accordance with the terms and principles set out in the MSA.

18. DISPUTE RESOLUTION

Any dispute, difference or claim arising out of or in connection with the Agreement which is not resolved amicably shall be decided in accordance with the dispute resolution procedure as set out in the MSA.

19. MISCELLANEOUS

a) Assignment and charges

This Agreement shall be binding on and ensure for the benefit of each Party’s successors in title. No Party shall assign, or declare any trust in favour of a third party over, all or any part of the benefit of, or its rights or benefits under, this Agreement.

b) Governing law and jurisdiction

This Agreement shall be construed and interpreted in accordance with and governed by the laws of India, and the courts at the State of ----------- shall have jurisdiction over matters arising out of or relating to this Agreement.

c) Waiver of sovereign immunity

The Parties unconditionally and irrevocably:

i. agree that the execution, delivery and performance by them of the Agreement constitute commercial acts done and performed for commercial purpose;

ii. agree that, should any proceedings be brought against a Party or its assets, property or revenues in any jurisdiction in relation to the Agreement or any transaction contemplated by the Agreement, no immunity (whether by reason of sovereignty or otherwise) from such proceedings shall be claimed by or on behalf of such Party with respect to its assets;

iii. waive any right of immunity which it or its assets, property or revenues now has, may acquire in the future or which may be attributed to it in any jurisdiction; and

iv. consent generally to the enforcement of any judgment or award against it in any such proceedings to the giving of any relief or the issue of any process in any jurisdiction in connection with such proceedings (including the making, enforcement or execution against it or in respect of any assets, property or revenues whatsoever irrespective of their use or intended use of any order or judgment that may be made or given in connection therewith).

d) Variation

This Agreement may only be varied in writing and signed by both Parties.

e) Waiver

i. Waiver including partial or conditional waiver, by either Party of any default by the other Party in the observance and performance of any provision of or obligations under this Agreement:-

- shall be in writing
- shall not operate or be construed as a waiver of any other or subsequent default hereof or of other provisions of or obligations under this Agreement;
- shall not be effective unless it is in writing and executed by a duly authorized representative of the Party; and
- shall not affect the validity or enforceability of this Agreement in any manner.

f) Exclusion of implied warranties

This Agreement expressly excludes any warranty, condition or other undertaking implied at law or by custom or otherwise arising out of any other agreement between the Parties or any representation by either Party not contained in a binding legal agreement executed by both Parties.

g) Survival

i. Termination or expiration of the Term shall:

- not relieve the Implementation Agency or the Buyer, as the case may be, of any obligations hereunder which expressly or by implication survive hereof; and
- except as otherwise provided in any provision of this Agreement expressly limiting the liability of either Party, not relieve either Party of any obligations or liabilities for loss or damage to the other Party arising out of, or caused by, acts or omissions of such Party prior to the effectiveness of such termination or expiration or arising out of such termination or expiration.

ii. All obligations surviving termination or expiration of the Term shall cease on termination or expiration of the Term.

h) **Entire Agreement**

This Agreement and the Annexure together constitute a complete and exclusive statement of the terms of the agreement between the Parties on the subject hereof, and no amendment or modification hereto shall be valid and effective unless such modification or amendment is agreed to in writing by the Parties and duly executed by persons especially empowered in this behalf by the respective Parties. All prior written or oral understandings, offers or other communications of every kind pertaining to this Agreement are abrogated and withdrawn.

i) **Severability**

If for any reason whatever, any provision of this Agreement is or becomes invalid, illegal or unenforceable or is declared by any court of competent jurisdiction or any other instrumentality to be invalid, illegal or unenforceable, the validity, legality or enforceability of the remaining provisions shall not be affected in any manner, and the Parties shall negotiate in good faith with a view to agreeing to one or more provisions which may be substituted for such invalid, unenforceable or illegal provisions, as nearly as is practicable to such invalid, illegal or unenforceable provision. Failure to agree upon any such provisions shall not be subject to the dispute resolution procedure set forth under this Agreement or otherwise.

j) **No partnership**

This Agreement shall not be interpreted or construed to create an association, joint venture or partnership between the Parties, or to impose any partnership obligation or liability upon either Party, and neither Party shall have any right, power or authority to enter into any agreement or undertaking for, or act on behalf of, or to act as or be an agent or representative of, or to otherwise bind, the other Party except as expressly provided under the terms of this Agreement.

k) **Third parties**

This Agreement is intended solely for the benefit of the Parties and their respective successors and permitted assigns, and nothing in this Agreement shall be construed to create any duty to, standard of care with reference to, or any liability to, any person not a Party to this Agreement.

l) **Notices**

Any notice or other communication to be given by any Party to the other Party under or in connection with the matters contemplated by this Agreement shall be in writing and shall be given by hand delivery, recognized courier, registered post, email or facsimile transmission and delivered or transmitted to the Parties at their respective addresses set forth below:

If to Purchaser:

Attn: <***>

Tel:

Fax:

Email:

Contact:

With a copy to:

If to the Implementation Agency:

Attn. <***>

Phone: <***>

Fax No. <***>

m) Language

All notices required to be given by one Party to the other Party and all other communications, documentation and proceedings which are in any way relevant to this Agreement shall be in writing and in the English language.

n) Counterparts

This Agreement may be executed in two counterparts, each of which, when executed and delivered, shall constitute an original of this Agreement.

o) Mitigation

Without prejudice to any express provisions of this Agreement on any mitigation obligations of the Parties, each of the Purchaser and the Implementation Agency shall at all times take all reasonable steps to minimize and mitigate any loss for which the relevant Party is entitled to bring a claim against the other Party pursuant to this Agreement.

p) Removal of Difficulties

The Parties acknowledge that it is conceivable that the Parties may encounter difficulties or problems in the course of implementation of the Project and the transactions envisaged under this Agreement. The Parties agree and covenant that they shall mutually discuss such difficulties and problems in good faith and take all reasonable steps necessary for removal or resolution of such difficulties or problems.

IN WITNESS WHEREOF THE PARTIES HAVE EXECUTED AND DELIVERED THIS AGREEMENT AS OF THE DATE FIRST ABOVE WRITTEN.

SIGNED, SEALED AND DELIVERED	SIGNED, SEALED AND DELIVERED
For and on behalf of the Implementation Agency by:	For and on behalf of the Purchaser by:
(Signature) (Name) (Designation) (Address) (Fax No.)	(Signature) (Name) (Designation) (Address) (Fax No.)

In the presence of:

1.

2.

ANNEXURE A – SERVICE LEVELS

Refer document - RFP Vol 3 - Annexure A (Service Levels)

Comptroller and Auditor General of India

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Request for Proposal

`Selection of System Integrator for Implementation, Rollout and Operations & Maintenance of

‘One IA&AD One System’ (OIOS) Project

VOLUME – III – Annexure A

Reference Number: 51-ISW/2019-‘One IA&AD One System’ Project

Contents

1 Annexure A: Service Levels

1.1 Purpose of this document

The purpose of this section is to clearly define the levels of service to be provided by SI to IA&AD for the duration of this project.

1.2 Description of Services Provided

SI shall provide services as defined in **Volume I** of this RFP.

1.3 Duration of SLA

1. The service level enforcement would begin post phase –I go-live
2. This SLA may be reviewed and revised according to the procedures detailed in the Service Level Agreement of this RFP.

1.4 SLA Specific Definitions

Prime Business Hours (PBH) - PBH refers to the prime business period, which shall be from 9:00 hrs till 18:00 hrs on Monday to Friday (excluding national public holidays, declared holidays and all Saturdays and Sundays).

Extended SLA Hours (ESH) - ESH refers to the non-business period, which shall be:

From 18:00 hrs till 9:00 hrs (next day) on Monday to Friday,

From 00:00 hrs to 23:59 hrs on Saturday, Sunday, National public holidays

Outages are the instance where users experience no response from the Application. Outages can be: I. Unplanned ii. Planned outage/ Scheduled Downtime

1. **Unplanned outage** is defined as an event caused without prior notice where users experience no response from an Application for whatsoever is the reason (within the scope of services of the SI).

   1. Planned outage/Scheduled Downtime:

      i. Pre-scheduled preventive maintenance and health checks (Scheduled outage).

ii. The SI must notify IA&AD via email of the upcoming maintenance at least Three (3) business days prior to Scheduled Downtime.

iii. It shall not be scheduled during prime business hours.

iv. Any planned / scheduled downtime shall not be more than 2 hours else it shall be considered unplanned outage and penalized accordingly.

v. The planned downtime would not be added to the SLA downtime unless it runs into prime business hours of the following day.

vi. Overall Planned downtime shall not be more than 24 hours in a quarter.

vii. The downtime for scheduled maintenance (patch application, upgrades – OS, Database, etc.) would need to be mutually agreed between IA&AD and the SI. To reduce this time, various maintenance activities can be clubbed together with proper planning.

Recording of outage period

1. The recording of outages shall commence at the time of:
    a) Registering the call with SI

    b) Auto alerts triggered through monitoring tools- in case of WAN or LAN and other infrastructure

    c) For any outage situation for the application / hardware.

2. Outages shall end when the problem is rectified and the application/ service is available to the user.

Contact for support /complaint will be by email or telephone. A Call will be logged by the SI/user in the System and an email/written response shall be provided to the system user about the resolution of the problem.

Uptime means, the aggregate number of hours in any specified time period during which application / hardware is actually available for use.

Uptime Calculation for the month:

{[(Uptime Hours + Scheduled Downtime) / Total No. of Hours in the time period] x 100}

Incident refers to any event / abnormalities in the functioning of the application / hardware that may lead to disruption in normal operations of the IA&AD.

Helpdesk Support shall mean the IT Help desk, which shall handle Fault reporting, Trouble Ticketing and related enquiries during this Project.

Help desk Resolution Time shall mean the time taken (after the incident has been reported at the help desk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level or to respective OEMs, getting the confirmatory details about the same from the OEM and conveying the same to the end user), the services related troubles during the first level escalation. The resolution time shall vary based on the severity of the incident reported at the help desk.

1.5 Service levels

This section is agreed to by IA&AD and SI as the key SI performance indicator for this engagement. It reflects the measurements to be used to track and report level of service on a regular basis. The targets shown in the following sub-sections are for the period of contract or its revision whichever is later.

1.5.1 Team Mobilization

Definition and Description	**Team mobilization and submission of final project plan**
Service Level Requirement	SI to mobilize the team: **Within 15 days from Contract signing date:** 1. Key resources as identified in RFP Vol-I, II **Within 3 weeks from Contract signing date:** 1. Minimum 50% of the Development Team

<table>
<tr><th>Definition and Description</th><th>Team mobilization and submission of final project plan</th></tr>
<tr><td></td><td><b>Within 5 weeks from Contract signing date:</b> Full Team as per proposal submitted by SI.
If the team mobilization exceeds 8 weeks from the Contract signing date, then IA&AD reserves the right to terminate the agreement.</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>To be measured in Number of days of delay from the date of signing of the MSA.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>
<table>
<tr><th>Delay in Team Mobilization</th><th>Liquidated Damages</th></tr>
<tr><td><b>>3 days and <= 10 days</b></td><td>0.01 % of Total Contract Value</td></tr>
<tr><td><b>>10 days and <= 20 days</b></td><td>0.02 % of Total Contract Value</td></tr>
<tr><td><b>>20 days</b></td><td>0.05 % of Total Contract Value</td></tr>
</table>
</td></tr>
</table>

1.5.2 Change in named Key Personnel

Definition and Description	Key Personnel team deputed on the project to consist of same members whose names were proposed in the bid/Project Start.
Service Level Requirement	There should not be any deviation in Key personnel whose names were proposed in the bid/Project Start
Measurement of Service Level Parameter	No change in the proposed Key personnel[1] except with prior approval of IA&AD.
Penalty for non-achievement of SLA Requirement	

[1] Except if the personnel resigns from his/her organisation or due to medical incapacity

<table>
<tr><th>Definition and Description</th><th>Key Personnel team deputed on the project to consist of same members whose names were proposed in the bid/Project Start.</th></tr>
<tr><td></td><td>
<table>
<tr><th>Number of Key personnel Changed without prior approval</th><th>Liquidated Damages</th></tr>
<tr><td><b>1 (not including Project Manager)</b></td><td>0.001% of Total Contract Value</td></tr>
<tr><td><b>2 to 4</b></td><td>0.002% of Total Contract Value</td></tr>
<tr><td><b>4 to 6</b></td><td>0.004% of Total Contract Value</td></tr>
</table>
For each additional change, Liquidated Damages of Value will be levied as additional Liquidated Damages.
In case of Project Manager recommended for the assignment is changed an additional Liquidated Damages of 0.015% of the Total Contract Value will be levied.
</td></tr>
</table>

1.5.3 Delay in any of the Project Milestones

<table>
<tr><th>Definition and Description</th><th>All the Project Milestones as defined in the RFP under Project Timelines should be completed within the defined timelines</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>All the Project Milestones as defined in the RFP under Project Timelines should be completed within the defined timelines.</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>Measured as the difference between the planned date for the milestone and the actual date of its completion.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>
<table>
<tr><th>Delay in Project milestones</th><th>Liquidated Damages as % of the value of the track / phase to which the deliverable pertains</th></tr>
<tr><td><b>&gt;7 days to <=10 days</b></td><td>0.5%</td></tr>
<tr><td><b>&gt;10 days to <=15 days</b></td><td>1%</td></tr>
<tr><td><b>&gt;15 days to <=20 days</b></td><td>2%</td></tr>
</table>
</td></tr>
</table>

Definition and Description	All the Project Milestones as defined in the RFP under Project Timelines should be completed within the defined timelines
	For each additional week or part thereof after 20 days, Liquidated Damages of 3% will be levied as additional Liquidated Damages.

1.5.4 Delay in setting up of DC-DR

<table>
<tr><th>Definition and Description</th><th>All the Project Milestones as defined in the RFP under Project Timelines should be completed within the defined timelines</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>Migration of development & UAT environment to Tier-3 co-located DC/DR to be completed as per project milestone</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>Measured as the difference between the planned date for the milestone and the actual date of its completion.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>Any additional cost for continuing development & UAT in cloud environment shall be borne by the SI, in addition to penalty:
<table>
<tr><th>Delay in Project milestones</th><th>Liquidated Damages as % of the value of the track / phase to which the deliverable pertains</th></tr>
<tr><td><b>&gt;7 days to <=10 days</b></td><td>0.5%</td></tr>
<tr><td><b>&gt;10 days to <=15 days</b></td><td>1%</td></tr>
<tr><td><b>&gt;15 days to <=20 days</b></td><td>2%</td></tr>
</table>
For each additional week or part thereof after 20 days, Liquidated Damages of 3% will be levied as additional Liquidated Damages.</td></tr>
</table>

1.5.5 Delay in Phase 1 Go-live date

Definition and Description	Design, Development and implementation of Phase 1 Go-Live as per the timelines defined in the RFP
Service Level Requirement	Design, Development and implementation of Phase 1 Go-Live as per the timelines defined in the RFP

<table>
<tr><th>Definition and Description</th><th>Design, Development and implementation of Phase 1 Go-Live as per the timelines defined in the RFP</th></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>Measured as the difference between the Planned Date for Go-Live and the Actual date of Go-Live</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td><table>
<tr><th>Delay in Project milestones</th><th>Liquidated Damages as % of the Total Contract Value</th></tr>
<tr><td><b>&gt;10 days to <=15 days</b></td><td>0.10%</td></tr>
<tr><td><b>&gt;15 days to <=20 days</b></td><td>0.25%</td></tr>
<tr><td><b>&gt;20 days to <=25 days</b></td><td>0.40%</td></tr>
</table>With each additional day of delay after 25 days, Liquidated Damages of 0.10% will be levied as additional Liquidated Damages.</td></tr>
</table>

1.5.6 Manpower Deployment during Phase 3

<table>
<tr><th>Definition and Description</th><th>Resource Deployment for Phase 3</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>SI to deploy all the resources (as agreed with IA&AD) for Phase 3 within the timelines defined in the RFP.
If the team mobilization exceeds 8 weeks, then IA&AD reserves the right to terminate the agreement.</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>To be measured as the difference between the planned date for the Resources Deployment and the actual date of its completion.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td><table>
<tr><th>Delay in Team Mobilization</th><th>Liquidated Damages</th></tr>
<tr><td>&gt;15 days and <= 20 days</td><td>0.01 % of Total Contract Value</td></tr>
<tr><td>&gt;20 days and <= 30 days</td><td>0.02 % of Total Contract Value</td></tr>
<tr><td>&gt;30 days</td><td>0.05 % of Total Contract Value</td></tr>
</table></td></tr>
</table>

1.5.7 Availability of SLA Monitoring Tool

In absence of SLA Monitoring tool, all the other SLAs shall be considered as Zero and respective Liquidated Damages shall be applicable.

1.5.8 OIOS Production Server Availability

<table>
<tr><th>Definition and Description</th><th>Availability refers to the total time when the VM is available to the users for performing all activities and tasks.</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>The average availability of the VM (at DC/DR level) for hosting:
1. OIOS application
2. Analytics
3. DR services as and when activated
4. Security and EMS tools as applicable
Quarterly average shall be at least 99.9% in a quarter.</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>Uptime = [(Total Availability of the Servers in a quarter)/ (Total Time in a quarter]*100
Any planned downtime shall NOT be included in the calculation of availability.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>If the System Integrator is not able to meet the above defined service level requirement, then any deviation from the same would attract a penalty as per the following :
<table>
<tr><th>Server/ VM Availability</th><th>&gt;= 99.5 % to &lt; 99.9%</th><th>&gt;= 99.5% to &lt; 99%</th><th>&lt; 99%</th></tr>
<tr><td>Penalty</td><td>0.5% of quarterly payment</td><td>1% of quarterly payment</td><td>2% of quarterly payment</td></tr>
</table>
If the Server availability is consistently below 99% for five days or more in a quarter, then IA&AD will have the right to terminate the MSA.</td></tr>
</table>

1.5.9 OIOS Application Availability

<table>
<tr><th>Definition and Description</th><th>Uptime would be measured as total time in minutes in a quarter minus the downtime in minutes in the quarter. However, in calculating downtime, scheduled downtime will not be considered.</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>Uptime shall be minimum 99.9 % per quarter.</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>The uptime and downtime shall be monitored for all the OIOS Application and Associated Components accessible over intranet & internet.
The System Integrator shall provide tools / mechanisms to measure the same. The tool / mechanism should be able to provide IA&AD information about downtime and historical information about the same.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>If the System Integrator is not able to meet the above defined service level requirement, then any deviation from the same would attract a penalty as per the following –
<table>
<tr><th>Application uptime (Quarterly average)</th><th>&gt;= 99 % to &lt; 99.9%</th><th>&gt;= 97% to &lt; 99%</th><th>&lt; 97%</th></tr>
<tr><td>Penalty</td><td>0.5% of quarterly payment of Operations and Maintenance</td><td>1% of quarterly payment of Operations and Maintenance</td><td>2% of quarterly payment of Operations and Maintenance</td></tr>
</table>
If the Application is consistently below 97% during PBH continuously for five days or more in a quarter, then IA&AD will have the right to terminate the MSA.</td></tr>
</table>

1.5.10 OIOS Support Services

<table>
<tr><th>Definition and Description</th><th>Availability of all OIOS Components supplied as support services to OIOS</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>Uptime shall be minimum 99.9 % per quarter.</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>The uptime and downtime shall be monitored for all the supporting services of OIOS such as Database, Applications, Web Server, DMS, and BPM.
The System Integrator shall provide tools / mechanisms to measure the same. The tool / mechanism should be able to provide IA&AD information about downtime and historical information about the same.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>If the System Integrator is not able to meet the above defined service level requirement, then any deviation from the same would attract a penalty as per the following –
<table>
<tr><th>Application uptime (Quarterly average)</th><th>>= 99 % to < 99.9%</th><th>>= 97% to < 99%</th><th>< 97%</th></tr>
<tr><td>Penalty</td><td>0.5% of quarterly payment of Operations and Maintenances</td><td>1% of quarterly payment of Operations and Maintenances</td><td>2% of quarterly payment of Operations and Maintenances</td></tr>
</table>
If the services are consistently below 97% during PBH continuously for five days or more in a quarter, then IA&AD will have the right to terminate the MSA.</td></tr>
</table>

1.5.11 OIOS Application Response Time

Definition and Description	OIOS Application Response Time
Service Level Requirement	The application response time at DC/DR location should not exceed 2 Seconds.
Measurement of Service Level Parameter	Application response time will be measured on the basis of automated reports. Response time shall be measured on a minimum of 5 functionalities post login on the OIOS application. These functionalities shall be identified before start of O&M Phase. The data should be captured through automated tools 4 times in a day during the business hours. Any scheduled downtime should not be included in the calculation of application response time
Penalty for non-achievement of SLA Requirement	If Response time exceeds 3 sec – 0.1% per second per request of quarterly payment of Operations and Maintenances

1.5.12 OIOS Application - Documents Open/Download/ Upload

Definition and Description	OIOS Application - Documents Open/Download/ Upload
Service Level Requirement	Documents stored in DMS/Document Repository, should Open/download through OIOS application: • 2 MB within 5 Seconds • 10 MB within 8 Seconds Same timelines for Upload
Measurement of Service Level Parameter	Application response time will be measured on the basis of automated reports. All measurements will be at DC/DR. The data should be captured through automated tools 4 times in a day during the business hours. Any scheduled

Definition and Description	OIOS Application - Documents Open/Download/ Upload
	downtime should not be included in the calculation of application response time.
Penalty for non-achievement of SLA Requirement	If Average Quarterly Document view/download/ upload time exceeds 5 seconds– 0.1% Per Second Per Request of Quarterly Payment of Operations and Maintenances

1.5.13 RTO

<table>
<tr><th>Definition and Description</th><th>RTO at DC DR</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>RTO (Applicable for both unplanned eventuality and a planned DC – DR drill) shall be less than or equal to 4 hours</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>Time taken to recover all services to a defined recovery level from the time eventuality is declared.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>If the System Integrator is not able to meet the above defined service level requirement, then any deviation from the same would attract a penalty as per the following –
<table>
<tr><th colspan="2">Disaster Incident</th></tr>
<tr><td><b>Disaster Incident</b>
RTO (Applicable for both unplanned eventuality and a planned DC – DR drill)</td><td>1 % of quarterly payment of Operations and Maintenances</td></tr>
</table>
</td></tr>
</table>

1.5.14 Database/Applications/Web Server Performance

Definition and Description	Database/Applications/Web Server Performance will be assessed in terms of CPU utilization of VM and memory utilization.
Service Level Requirement	a. Average CPU Utilization (of VM) over any hour, measured at 5 minute intervals, shall not exceed 60% *. b. Average Memory Utilization over any hour, measured at 5 minute intervals, shall not exceed 60% *. *During disaster, at the time of failback from DC to DR, the Database/Applications/Web Server Performance parameters part of this SLA won't apply
Measurement of Service Level Parameter	Average Server utilization % of CPU/Memory Utilization in a month shall be monitored. The data shall be captured through automated tools every **5 minutes**. For an hour, average of 12 recorded data shall be taken into account. Multiple non-compliances in a 24 hr interval will be counted once only for penalty calculation purpose. Both noncompliance, CPU & Memory Utilization, occurring at the same event shall be considered single for calculation.

<table>
<tr>
<td><b>Penalty for non-achievement of SLA Requirement</b></td>
<td>If the System Integrator is not able to meet the above defined service level requirement, then any deviation from the same would attract a penalty as per the following –
<table>
<tr><th>Average CPU Utilization</th><th>&gt; 60 % to &lt;70%</th><th>&gt;= 70% to &lt;80%</th><th>&gt;=80%</th></tr>
<tr><td>Penalty</td><td>0.5 % of quarterly payment of Operations and Maintenances</td><td>2 % of quarterly payment of Operations and Maintenances</td><td>4 % of quarterly payment of Operations and Maintenances</td></tr>
</table>
<table>
<tr><th>Average Memory Utilization</th><th>&gt; 60 % to &lt;70%</th><th>&gt;= 70% to &lt;75%</th><th>&gt;=75%</th></tr>
<tr><td>Penalty</td><td>0.5 % of quarterly payment of Operations and Maintenances</td><td>2 % of quarterly payment of Operations and Maintenances</td><td>4 % of quarterly payment of Operations and Maintenances</td></tr>
</table>
</td>
</tr>
</table>

1.5.15 I/O Utilization

<table>
<tr><th>Definition and Description</th><th>I/O Utilization</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>Sustained periods of peak I/O utilization of any VM/storage crossing 70% shall be less than or equal to 30 minutes.</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>Each occurrence where the peak I/O utilization of any VM crosses 70% and stays above 70% for time more than 30 minutes will be treated as one instance.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>If the System Integrator is not able to meet the above defined service level requirement, then any deviation from the same would attract a penalty as per the following –
<table>
<tr><th colspan="2">Incident</th></tr>
<tr><td>number of incidents in respective quarter:</td><td></td></tr>
<tr><td>>0 & <=3</td><td>1 % of quarterly payment of Operations and Maintenances</td></tr>
<tr><td>>3</td><td>2 % of quarterly payment of Operations and Maintenances</td></tr>
</table>
</td></tr>
</table>

1.5.16 Security Incident Management

Definition and Description	Security being one of the most important aspects of IA&AD would be governed by stringent standards. All security incidents leading to disruption in services availability would be penalized heavily. Security incidents could consist of any of the following : Malware Attack: This shall include Malicious code infection of any of the VM in use for IA&AD or Unchecked malware infected mails passing through the Messaging solution.

	Denial of Service Attack: **This shall include non-availability of service (messaging service and other web services, etc. due to attacks that consumes related resources). The SI shall be responsible for monitoring, detecting and resolving all Denial of Service (DoS).** **Intrusion:** **Successful Unauthorized access to IA&AD system, resulting in a loss of confidentiality/Integrity/availability of data. The SI shall be responsible for monitoring, detecting and resolving all security related intrusions on the network using an Intrusion Prevention device.**
Service Level Requirement	a. Any Denial of service attack shall not lead to complete service non-availability. b. Desired service level shall not allow even a single web defacement, data theft and Intrusion. Each occurrence of these three types of security violation shall lead to appropriate penalties as mentioned below.
Measurement of Service Level Parameter	The network shall be monitored for: **Malware Attack:** Any malware infection and passing of malicious code through messaging solution shall be monitored at the gateway level or user complaints of malware infection shall be logged in the help desk system and collated every quarterly. Logs will be monitored every quarterly. a. The SI has to ensure that all the servers/computers (in scope) have anti-malware installed with the latest pattern files. b. Real-time scan has to be enabled on all systems and users shall not be given the option of being able to uninstall the anti-malware client or stop a scheduled scan. c. All clients shall be configured to receive the latest pattern file from the central anti-malware server.

	d. The SI shall configure the AV system to perform scheduled scans every day/week at a time decided mutually with IA&AD. **Denial of Service Attack:** Non availability of any services shall be analysed and forensic evidence shall be examined to check whether it was due to external DoS attack. **Security:** The SI will be responsible to install and maintain security components at DC and DR and project locations as per the requirements of the RFP. **Intrusion:** Compromise of any kind of data hosted by IA&AD. **Multiple non-compliances for each Incident Type in an 24 hr interval will be counted one incident only for penalty calculation purpose.** Note: Forensic evidence shall be analysed for all incidents

Penalty for non-achievement of SLA Requirement	If the System Integrator is not able to meet the above defined service level requirement, then any deviation from the same would attract a penalty as per the following –

Security Incident	
Security Incident (Malware Attack/ Denial of Service Attack/ Data Theft/ Loss of data/ Intrusion or Defacement)	1 % of quarterly payment of Operations and Maintenances

Uptime of Security Components (100% uptime for SIEM,IDS/IPS, Antimalware - beyond planned downtime) (quarterly average)	**>= 99 % to < 99.9%**	**>= 97% to < 99%**	**< 97%**
Penalty	2% of quarterly payment of Operations and Maintenances	15% of quarterly payment of Operations and Maintenances	25% of quarterly payment of Operations and Maintenances

1.5.17 Security Components Availability

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>ISO 27001</b></td><td>Within 18 months of Go Live</td><td>To achieve the desired certification for OIOS system</td><td>
<table>
<tr><td>Time for achieving ISO 27001 certification</td><td>Liquidated damaged as % of the quarterly payments during the Operations & Maintenance Phase& Maintenance Phase</td></tr>
<tr><td>&gt;547 days & <=570 days</td><td>0.5%</td></tr>
<tr><td>&gt;570 days & <=600 days</td><td>1%</td></tr>
<tr><td>&gt;600 days & <=630 days</td><td>2%</td></tr>
</table>
For each additional 30 days after 630 days 1% of quarterly payment will be levied as additional liquidated damages.
</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th colspan="2">Liquidated Damage</th></tr>
<tr><td rowspan="5"><b>ISO 22301</b></td><td rowspan="5">Within 18 months of Go Live</td><td rowspan="5">To achieve the desired certification for OIOS system</td><td>Time for achieving the ISO 22301 certification</td><td>Liquidated damaged as % of the quarterly payments during the Operations & Maintenance Phase& Maintenance Phase</td></tr>
<tr><td>&gt;547 days & <=570 days</td><td>0.5%</td></tr>
<tr><td>&gt;570 days & <=600 days</td><td>1%</td></tr>
<tr><td>&gt;600 days & <=630 days</td><td>2%</td></tr>
<tr><td colspan="2">For each additional 30 days after 630 days 1% of quarterly payment will be levied as additional liquidated damages.</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Average uptime for the Security components at the DC/DR / other sites</b></td><td>Measured as the percentage of time the Components at DC/DR / Other sites is up and running on a monthly basis. This will be measured on 24X7 basis</td><td>>=99.9%</td><td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>% Uptime</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td><b><99.9% & >=99%</b></td><td>0.5%</td></tr>
<tr><td><b>< 99% & >= 98%</b></td><td>1%</td></tr>
<tr><td><b>< 98% & >= 97%</b></td><td>2%</td></tr>
</table>
For each additional drop of <i>1%</i> in performance below 97%, <i>1% of</i> Quarterly payment of Operations & Maintenance will be levied as additional liquidated damages.</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Security reporting</b></td><td>MIS report to be submitted on quarterly basis within pre-defined timelines
100% reporting of the security KPI’s (defined during project start)</td><td>100% on time reporting</td><td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>Delay in submission of Security-Reporting
MIS report</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td><b>&gt; 1 day &amp; < = 5 days</b></td><td><b>0.5%</b></td></tr>
<tr><td><b>&gt; 5 days & <= 10 days</b></td><td><b>1%</b></td></tr>
<tr><td><b>&gt; 10 day's & <= 15 days</b></td><td><b>2%</b></td></tr>
</table>
For each additional week after 15 days, 1% of Quarterly payment will be levied as additional liquidated damages.</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Anti-virus signature update</b></td><td>Availability of latest AV signature on the GST system components</td><td>Latest AV signature to be installed on at least 98% of all applicable components within 6 hours</td><td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>Delay in Vulnerability assessment and closure of vulnerabilities after due date (in days)</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td><b>>= 97% & < 98%</b></td><td>0.5%</td></tr>
<tr><td><b>>= 96% & < 97%</b></td><td>1%</td></tr>
<tr><td><b>>= 95% & < 96%</b></td><td>2%</td></tr>
</table>
For each additional drop in percentage after 95%, 1% of Quarterly payment will be levied as additional liquidated damages</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Vulnerability assessment and closure</b></td><td>Six monthly</td><td>Vulnerability Assessment for all systems / sub systems / Network devices shall be performed once every six months and all detected vulnerabilities closed within the cycle.</td><td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>Delay in Vulnerability assessment and closure of vulnerabilities after due date (in days)</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td><b>&gt;= 10 &amp; &lt; 20</b></td><td>0.5%</td></tr>
<tr><td><b>&gt;= 20 &amp; &lt; 30</b></td><td><b>1%</b></td></tr>
<tr><td><b>&gt;=3O&amp;&lt;35</b></td><td>2%</td></tr>
</table>
For each additional week delay beyond 35 days, 1% of Quarterly payment will be levied as additional liquidated damages</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Penetration testing</b></td><td>Yearly</td><td>Penetration Testing (external) will be conducted once every year. All detected vulnerabilities to be closed within the year.</td><td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>For each additional week’s delay beyond 45 days, 1% of Quarterly payment will be levied as additional liquidated damages
<b>Delay in penetration testing and closure of detected vulnerabilities after due date (in days)</b></th><th><b>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</b></th></tr>
<tr><td><b>>= IO & < 30</b></td><td>0.5%</td></tr>
<tr><td><b>>= 30 & < 40</b></td><td><b>1%</b></td></tr>
<tr><td><b>>= 40 & < 45</b></td><td>2%</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr>
<td><b>Reporting of Security Incidents</b></td>
<td>Any incident wherein system compromised or any actual or reasonably suspected unauthorized use of or access to provider systems or any case wherein data theft occurs (including internal incidents)</td>
<td>The provider to investigate the breach, use its best efforts to mitigate the breach’s impact, collect evidence surrounding the breach, and document its response.</td>
<td>For each breach/data theft, liquidated damages will be levied as per following criteria.
<table>
<tr><th>Delay in Mitigating of Security Breaches</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td>Failure to Mitigate and document the response.</td><td>1 %</td></tr>
</table>
This liquidated damage is applicable per breach. These liquidated damages will be in addition to the SLA liquidated damages cap per quarter.
In case of serious breach of security wherein the data is stolen or corrupted, CAG reserves the right to terminate the contract</td>
</tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Security breach including Data Theft/Loss/ Corruption</b></td><td>Any incident wherein system compromised or any actual or reasonably suspected unauthorized use of or access to provider systems or any case wherein data theft occurs (including internal incidents)</td><td>The provider to Detect the breach and Report on the details and impact of the same to IAAD environment</td><td>For each breach/data theft, liquidated damages will be levied as per following Criteria.
<table>
<tr><th>Delay in Detecting and reporting of Security Breaches</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td>&gt; 15 mins & < = 30 mins</td><td>0.5%</td></tr>
<tr><td>&gt; 30 mins & <= 1 hours</td><td>1%</td></tr>
</table>
This liquidated damage is applicable per breach. These liquidated damages will be in addition to the SLA liquidated damages cap per quarter.
In case of serious breach of security wherein the data is stolen or corrupted, CAG reserves the right to terminate the contract.</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr>
<td><b>Patch updates</b></td>
<td>Availability of latest patches on the IAAD system components</td>
<td>All patches released, to be installed on at least 98% of all applicable components</td>
<td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>Percentage of system components on which latest patches are installed</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td><b>>= 97% & < 98%</b></td><td><b>0.5%</b></td></tr>
<tr><td><b>>= 96% & < 97%</b></td><td>1%</td></tr>
<tr><td><b>>= 95% & < 96%</b></td><td>2%</td></tr>
</table>
For each additional drop in percentage after 95%, 1% of Quarterly payment will be levied as additional liquidated damages</td>
</tr>
</table>

1.5.18 Help Desk Resolution Time

Definition and Description	**Time in which a complaint / query is resolved after it has been reported to the helpdesk team of the System Integrator.**
Service Level Requirement	The helpdesk agents are required to be available physically only during PBH. Any query (other than functional/domain queries) after being given a response shall be classified for resolution in following four categories. Categorization of the queries / issues while may be done by the SI team but subject to review and modification by the IA&AD monitoring team. **Resolution Level 1 (R1):** Queries regarding issues which have the greatest business impact wherein the user is not able to perform his/her regular work. For example, unable to login to the system due to errors in software, critical module not working etc. **Resolution Level 2 (R2):** Queries regarding issues which have a medium business impact wherein the user is partially able to perform his/her regular work. For example, the user is able to login and perform most of his normal work, but can't approve a certain request through the system. **Resolution Level 3 (R3):** Queries regarding issues which have the least/no business impact involving cosmetic changes. For example, text alignment issues, change of background colour etc. **Resolution Level 3 (R4):** Queries regarding enhancement requests. For example, the addition of new functionality, etc. (IA&AD will collate and review the enhancement requests and initiate Change control process accordingly) The System Integrator shall provide services as per the following standards –

<table>
<tr><th>Definition and Description</th><th>Time in which a complaint / query is resolved after it has been reported to the helpdesk team of the System Integrator.</th></tr>
<tr><td></td><td><table>
<tr><th>Type of Query</th><th>Maximum resolution time allowed</th><th>Performance baseline</th></tr>
<tr><td>R1</td><td>4 business hours</td><td>All calls resolved within defined timeline</td></tr>
<tr><td>R2</td><td>8 business hours</td><td>At least 99.5% calls resolved within defined timeline</td></tr>
<tr><td>R3</td><td>16 business hours</td><td>At least 98% calls resolved within defined timeline</td></tr>
<tr><td>R4</td><td>To be calculated in discussion with IA&AD on case by case basis.</td><td></td></tr>
</table></td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>The service level would be defined in the number of business hours calculated from the date & time of logging the call/raising the request with the System Integrator.
The System Integrator shall provide help desk software / tools / mechanisms to measure the same. The tool / mechanism shall be able to provide IA&AD information about Help Desk Resolution Time, and historical information about the same. After categorizing the Response Type, this shall be appropriately entered into the Helpdesk Log.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>Delay of every Business Hour would attract a penalty per hour as per the following –
1. For Each R1 = 5 X Per hour Penalty (The Penalty per hour is INR 1000)</td></tr>
</table>

Definition and Description	Time in which a complaint / query is resolved after it has been reported to the helpdesk team of the System Integrator.
	2. For Each R2 = 3 X Per hour Penalty (The Penalty per hour is INR 1000) 3. For Each R3 = 1 X Per hour Penalty (The Penalty per hour is INR 1000) Note: after the lapse of the resolution time, the query / issue should be escalated as per the escalation matrix submitted by the bidder.

1.5.19 Percentage of Re-opened incidents

<table>
<tr><th>Definition and Description</th><th>All the incidents which are designated Resolved by the SI, but are re-opened by the client.</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>For any quarter, no. of Re-opened incidents should not be &gt; 2%</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>Re-opened incidents = No. of incidents re-opened in the quarter * 100/ No. of Incidents logged in the quarter</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>
<table>
<tr><th>% of Re-opened incidents</th><th>Liquidated Damages as % of the quarterly payments during O&M Phase</th></tr>
<tr><td>&gt;2% and &lt;=4%</td><td>0.5%</td></tr>
<tr><td>&gt;4% and &lt;=6%</td><td>1%</td></tr>
<tr><td>&gt;6% and &lt;=8%</td><td>2%</td></tr>
<tr><td>&gt;8%</td><td>5%</td></tr>
</table>
</td></tr>
</table>

1.5.20 Backup and Archival Management

<table>
<tr><th>Definition and Description</th><th>The System Integrator shall take backup as per the backup and archival policy (to be finalised in discussion with IA&AD).</th></tr>
<tr><td><b>Service Level Requirement</b></td><td>The System Integrator shall take backup of data, email and logs. Given below is indicative backup and archival policy. The actual policy will be discussed and finalised in discussion IA&AD.
a. Incremental backup – every four hours
b. Full backup shall be taken on specific media once in a week.
c. Two (2) weeks data backup must be available at any time.
d. Full data shall be archived once a month (Interval between two archives not to exceed five weeks).
e. Testing of the backup will be undertaken by SI once every quarter for all three months.</td></tr>
<tr><td><b>Measurement of Service Level Parameter</b></td><td>SI shall adhere the backup and archival schedule/frequency to at least 99%. The parameter will be calculated on a quarterly basis.</td></tr>
<tr><td><b>Penalty for non-achievement of SLA Requirement</b></td><td>
<table>
<tr><th>Data and mail backup</th><th>>= 98 % to < 99%</th><th>>= 96% to < 98%</th><th>< 96%</th></tr>
<tr><td>Penalty</td><td>0.25 % of quarterly payment</td><td>0.5 % of quarterly payment</td><td>1 % of quarterly payment</td></tr>
</table>
</td></tr>
</table>

1.5.21 Performance

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>DR Drills</b></td><td>Number of drills as per the defined policy or at least two DR drills in a year (once every six months)</td><td>On time</td><td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>No. of DR drills</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td><b>1</b></td><td>1%</td></tr>
<tr><td><b>0</b></td><td>2%</td></tr>
</table>
These will be measured every six months and the liquidated damages will be levied in the quarter following the end of the six month period Note: Since both the DC are planned to be deployed in active-active mode the modalities for implementation of this SLA will be discussed and finalized with the selected MSP.</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Bandwidth Link - packet drops (individual links)</b></td><td>Bandwidth Link - packet drops at DC/DR/NIC Net location</td><td>&lt;1%</td><td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>% of packet drops</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td><b>&lt; 1.5% &amp; &gt; 1%</b></td><td>0.5%</td></tr>
<tr><td><b>&lt; 2% &amp; &gt; = 1.5%</b></td><td><b>1%</b></td></tr>
<tr><td><b>&lt;= 2.5% &amp; &gt;= 2%</b></td><td>2%</td></tr>
</table>
For each additional drop of 0.5% in performance below 2.5%, 1% of Quarterly payment will be levied as additional liquidated damages.
Note: This liquidated damage to be calculated for each link</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Bandwidth Latency</b></td><td>Bandwidth Latency measured at DC/DR/NIC Net location</td><td><100 ms</td><td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>Average bandwidth latency (In milliseconds)</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td><b><120 & >= 100</b></td><td>0.5%</td></tr>
<tr><td><b><150 & >= 120</b></td><td><b>1%</b></td></tr>
<tr><td><b><200 & >= 150</b></td><td>2%</td></tr>
</table>
For each additional drop of 100 milliseconds in performance, 3% of Quarterly payment of Operation and Maintenance cost will be levied as additional liquidated damages.
Note: This liquidated damage to be calculated for each link</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Bandwidth Link Availability</b></td><td>Bandwidth link availability at DC/DR/NIC Net</td><td>Minimum 99.5% on quarterly basis</td><td>Liquidated damages will be levied as per the following table:
<table>
<tr><th>% of throughput observed</th><th>Liquidated damages as % of the Quarterly payments during Operations & Maintenance Phase</th></tr>
<tr><td><b>< 99.5% & > = 99%</b></td><td>0.5%</td></tr>
<tr><td><b>< 99% & > = 99.5%</b></td><td>1%</td></tr>
<tr><td><b>< 98% & > = 99%</b></td><td>2%</td></tr>
</table>
For each additional drop of 1% in performance below 98%, 1% of Quarterly payment will be levied as additional liquidated damages.
Note: This liquidated damage to be calculated for each link</td></tr>
</table>

<table>
<tr><th>SLA Parameter</th><th>Description</th><th>Target</th><th>Liquidated Damage</th></tr>
<tr><td><b>Change Management</b></td><td>Handling of change Requests</td><td>As per timelines defined in the Change Management section in the RFP or timelines agreed during the project</td><td>
<table>
<tr><th>Delay in change timelines</th><th>Liquidated Damages as % of the relevant cost of change</th></tr>
<tr><td><b>&gt;2 days to <=5 days</b></td><td>1%</td></tr>
<tr><td><b>&gt;5 days to <=10 days</b></td><td>2%</td></tr>
<tr><td><b>&gt;10 days to <=15 days</b></td><td>3%</td></tr>
</table>
With each additional delay after 15 days, Liquidated Damages of 02% will be levied as additional Liquidated Damages.</td></tr>
</table>

SLA Parameter	Description	Target	Liquidated Damage
Training and Capacity Building	Feedback to be taken from all attendees	>75% of training audience to give a satisfactory or above rating (per training)	In case session is rated Satisfactory or Excellent by less than 75 percent attendees, then the SI has to take the training session again. No extra payment would be due for re-training session

1.6 Others

1.6.1 SLA on additional services/items

Any additional/optional- equipment/service/items supplied by SI-as per the SI's commercial proposal (on IA&AD's request) shall also be governed by the terms and conditions set out in this agreement.

1.6.2 Installed Hardware

If any equipment supplied by SI fails for more than 3 times in a quarter OR for a total of more than 8 business hours in a quarter the SI will have to replace the equipment free of cost immediately.

1.6.3 Exclusions (for penalty calculation)

The SI will be exempted from any delays or slippages on SLA parameters arising out of the following reasons:-

1. The non-compliance with the SLA other than for reasons beyond the control of the SI. Any such delays will be notified in writing to IA&AD by SI, and will not be treated as a breach of SLA from the SI's point of view.
2. There is a force majeure event effecting the SLA which is beyond the control of the System Integrator.

1.6.4 SLA Monitoring and Auditing

IA&AD will review the performance of SI against the SLA parameters each quarter, or at any periodicity defined in this RFP document.

The review / audit report will form the basis of any action relating to imposing penalty or breach of terms and conditions of work order. Any such review /Audit can be scheduled or unscheduled. The results will be shared with the SI as soon as possible.

IA&AD reserves the right to appoint a third-party auditor to validate the SLA.

1.6.5 SLA Monitoring Tool

The System Integrator shall provide adequate tools for capturing data required for measuring SLAs at no extra cost to either IA&AD or IA&AD.

The Tool shall be tested and certified for its accuracy, reliability and completeness by IA&AD before it is deployed by SI.

The tools shall have the capability such that the IA&AD can log in anytime, without the involvement of SI, to see the status.

If the measurement tool and/or data equivalent to more than 5% of the sample size is missing or unavailable for a particular SLA metric or if the tool is found to be unreliable then the maximum penalty applicable against that metric will be applicable.

1.6.6 Reporting Procedures

The SI's representative will prepare and distribute SLA performance reports in an agreed upon format by the 10th calendar day / next working day of the subsequent quarter of the reporting period. Also, SI would be required to provide SLA performance report monthly for IA&AD records.

The reports will include "actual versus target" SLA performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports will be distributed to IA&AD.

1.6.7 Maximum Penalty to SI for the SLA

The maximum penalty levied (from the calculated penalty) at any point of time on an additive basis in any quarter shall not exceed 15% of quarterly payments due to the System Integrator. This is applicable only for the Operation and Maintenance phase.

1.6.8 Condition for termination

In case the calculated penalty exceeds 20%, for two consecutive quarters, IA&AD reserves the right to terminate the MSA.

1.6.9 Issue Management Procedures

This process provides an appropriate management structure for the orderly consideration and resolution of business and operational issues in the event that quick consensus is not reached between IA&AD and SI. It is expected that this pre-defined process will only be used on an exception basis if issues are not resolved at lower management levels.

1. Issue Management Process

1. Either IA&AD or SI may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.

IA&AD and the SI's representative will determine which committee or executive level shall logically be involved in resolution.

A meeting or conference call will be conducted to resolve the issue in a timely manner. The documented issues will be distributed to the participants at least 24 hours prior to the discussion if the issue is not an emergency requiring immediate attention.

Management of IA&AD and SI will develop a temporary, if needed, and the permanent solution for the problem at hand. The SI will then communicate the resolution to all interested parties.

In the event a significant business issue is still unresolved, the arbitration procedures described in the RFP document will be used.

2. Risk and Cost Factor

In the event of termination of the MSA on the basis of non-performance by the SI as per SLA, SI will be solely responsible for risk and cost factor thereon.

S .No	Form Reference	Track Name	Format Number	Project Component Name	Project Component Cost (INR)	Track Cost (INR)
1.	Format 3	**Track 1:** Setting Up of Development & Test Environment	Format 3A	Track 1 - Cloud Resource Cost Format	**₹ 0**	**₹ 0**
			Format 3B	Track 1: System Software Cost	**₹ 0**	
2.	Format 4	**Track 2:** OIOS Application Design, Development, Implementation and Rollout	Format 4A	OIOS Application Design, Development, Implementation and Rollout	**₹ 0**	**₹ 0**
			Format 4B	Track 2: Phase 1 Middleware and Software	**₹ 0**	
			Format 4C	Track 2: Phase 2 Middleware and Software	**₹ 0**	
			Format 4D	Phase 3 Development Team	**₹ 0**	
			Format 4E	OIOS Application Cloud to PDC Migration Cost	**₹ 0**	
3.	Format 5	**Track 3:** Setting Up of PDC and DRC and Backup Sites at 2 IA&AD offices	Format 5A	Track 3: Phase 1 - Setting Up of PDC	**₹ 0**	**₹ 0**
			Format 5B	Track 3: Phase 2 - Setting Up of PDC	**₹ 0**	
			Format 5C	Track 3: Phase 2 - Setting Up of DRC	**₹ 0**	
4.	Format 6	**Track 4:** Centralized Helpdesk Set Up and Operations			**₹ 0**	
5.	Format 7	**Track 5:** Training Cost			**₹ 0**	
6.	Format 8	**Track 6:** Operations and Maintenance Cost			**₹ 0**	
A.	**Total Cost (1+2+3+4+5+6) in Numbers**				**₹ 0**	
	Total Cost in Words: ***<<To be entered manually...>>***					

FORMAT 3A	Track 1 - Cloud Resource Cost Format							
#	**Item**	**Unit of Measurement**	**Quantity**	**Number of Months**	**Price Per Unit Per Month**	**Total Price (excluding taxes)**	**Tax in %age**	**Total Price (including taxes)**
			A	**B**	**C**	**D = A x B x C**	**E**	**F =D + (D x E/100)**
All Amount to be quoted in INR								
1	**VM (loaded with latest Linux or Windows environment which the bidder selects for development)**							
1.1.	X86 64Core with 256GB RAM	Number	1	3		0		0
Row Intentionally left Blank								
2.	**Storage**					0		0
2.1.	SSD 500 GB	Number	1	3		0		0
2.2.	SAS / NLSAS 500 GB	Number	1	3		0		0
Row Intentionally left Blank								
	Total Cost (In Numbers) Including Taxes							₹ 0
	Total Cost (In Words) Including Taxes	***<<To be entered manually...>>***						

FORMAT 3B			Track 1: System Software Cost													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
All Amount to be quoted in INR																
1	**Software development licenses for dev team**															
1.1.	Application Server		License			0		0								0
1.2.	Database Server		License			0		0								0
1.3.	BPM		License			0		0								0
1.4.	GIS		License			0		0								0
1.5.	Any other		License			0		0								0
	Total Cost (In Numbers) Including															***₹ 0***
	Total Cost (In Words) Including Taxes		***<<To be entered manually...>>***													

FORMAT 4A					
S No	Components Name	Unit	Total Capex (Excluding Taxes)	Taxes %	Total Capex (Inclusive of Taxes)
			A	B	C = A + (A*B/100)
All Amount to be quoted in INR					
A	OIOS Phase 1 - Bespoke Software Development	Lumpsum			0
B	OIOS Phase 2 - Bespoke Software Development	Lumpsum			0
Row Intentionally left Blank					
C	*Total Cost (In Numbers) Including Taxes*				*₹ 0*
	Total Cost (In Words) Including Taxes	*<<To be entered manually...>>*			

FORMAT 4B			Track 2: Phase 1 Middleware and Software													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
			Row Intentionally left Blank													
1.	**Supporting Platform**															
1.1.	Operating system – Open source		Support			0		0								0
1.2.	Operating system – COTS		License			0		0								0
1.3.	Virtualisation software		License/ CPU			0		0								0
1.4.	Virtualisation Manager Software		License/ Support	1		0		0								0
2.	**Core System Software Components**															
2.1.	Web server		Core	4		0		0								0
2.2.	Application Server		Core	4		0		0								0
2.3.	BPM Software		Core	4		0		0								0
2.4.	Document management system		Core	4		0		0								0
2.5.	Database – OIOS		Core	4		0		0								0
2.6.	Database security – OIOS		Core	4		0		0								0
2.7.	KMS Platform, discussion forum & Implementation		License	1		0		0								0
2.8.	Help desk Tool – OIOS		License	1		0		0								0
2.9.	Web conferencing tool (Helpdesk - multiple offices)		Host	10		0		0								0
2.10.	SIEM		License			0		0								0
2.11.	Identity access and management (for 29,000 users -25% delivery)		License			0		0								0
3.	**EMS Software**															
3.1.	Monitoring: IT Infrastructure (device based - OS Instances: Server OS, Virtualisation, Firewall, IPS, Storage)		Number			0		0								0
3.2.	Monitoring: OIOS Application Performance (Real User Monitoring, Diagnostics)		License			0		0								0
3.3.	Dashboard & Reporting (Events co-relation, Centralized Reporting)		License			0		0								0
3.4.	Service Desk (SLA monitoring, Incident Mgmt.)		License			0		0								0
3.5.	OIOS, IT Infrastructure Operational Analytics (Log Correlation & Analysis)		License			0		0								0
			Row Intentionally left Blank													
	Total Cost (In Numbers) Including Taxes															*₹ 0*
	Total Cost (In Words) Including Taxes		***<<To be entered manually...>>***													

FORMAT 4C			Track 2: Phase 2 Middleware and Software													
S No	Item	Proprietary / Open Source	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
			Row Intentionally left Blank													
1	**RDBMS Instance**															
1.1.	MySQL		Core	4		0		0								0
1.2.	PostgreSQL		Core	4		0		0								0
1.3.	MS SQL server		Core	4		0		0								0
1.4.	DB2		Core	4		0		0								0
1.5.	Oracle		Core	4		0		0								0
Row Intentionally left Blank																
	Total Cost (In Numbers) Including Taxes															***₹ 0***
	Total Cost (In Words) Including Taxes		***<<To be entered manually...>>***													

FORMAT 4D		Phase 3 Development Team					
S No	Resource Type	Quantity	Cost Per resource Per Month (Excluding Taxes)	Number of Months	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	C	D = A X B X C	E	F = D+(D*E/100)
All Amount to be quoted in INR							
1.	**Development Team**						
1.1.	Project Manager	1		18	0		0
1.2.	Scrum Master	3		18	0		0
1.3.	Enterprise Solution Architect	1		9	0		0
1.4.	Security Architect	1		6	0		0
1.5.	QC Expert	1		18	0		0
1.6.	Business Analyst	3		6	0		0
1.7.	Developers / Sr Developers	15		9	0		0
1.8.	UX/ UI Designer	3		18	0		0
1.9.	Test Lead	1		18	0		0
1.10.	Tester	3		18	0		0
1.11.	Data Preparation / Migration Expert	1		12	0		0
1.12.	Database Administrator	1		12	0		0
1.13.	System Administrator	1		18	0		0
Row Intentionally left Blank							
	Total Cost (In Numbers) Including Taxes						₹ 0
	Total Cost (In Words) Including Taxes	***<<To be entered manually...>>***					

FORMAT 4E	OIOS Cloud Development Environment to PDC Migration Cost				
S No	**Components Name**	**Unit**	**Total Cost (Excluding Taxes)**	**Taxes %**	**Total Cost (Inclusive of Taxes)**
			A	**B**	**C = A + (A*B/100)**
All Amount to be quoted in INR					
A	**Development environment Migration**	Lumpsum			0
B	**Network reconfiguration and connectivity with PDC**	Lumpsum			0
Row Intentionally left Blank					
C	***Total Cost (In Numbers) Including Taxes***				*₹ 0*
	Total Cost (In Words) Including Taxes	***<<To be entered manually...>>***			

FORMAT 5A			Track 3: Phase 1 - Setting Up of PDC													
S No	Item	Open Source / Proprietary	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
	Hardware components															
1.1.	Blade server chassis		Number	1		0		0								0
1.2.	Blade Servers with 2X16 cores (Total 96 Cores)		Number	3		0		0								0
1.3.	KVM Switch		Number	2		0		0								0
1.4.	SAN storage 40 TB Usable		License/ Support	1		0		0								0
1.5.	Racks		Number			0		0								0
1.6.	SAN Switch 24 Port		Number	2		0		0								0
1.7.	Access switch 10G		Number	4		0		0								0
1.8.	Structured Cabling within DC (Cat 6 A)		Job	1		0		0								0
Row Intentionally left Blank																
2.	**Security**															
2.1.	Firewall Next Generation with SSL VPN (1 GBPS cumulative throughput including 7.2, 7.3 and 7.4)		Number	2		0		0								0
2.2.	IPS		No	2		0		0								0
2.3.	Application Security		Subscription/Year	2		0		0								0
2.4.	URL filtering		Subscription/Year	2		0		0								0
2.5.	Anti-APT Solution with sand-boxing		Subscription/Year	1		0		0								0
2.6.	Web application firewall		No	2		0		0								0
2.7.	DLP (System administrators console)		License			0		0								0
2.8.	HIPS		License			0		0								0
2.9.	Privilege Management of System Administrator (VMs, Physical Servers, Storage)		LIC / VM			0		0								0
2.10.	Database Activity Monitoring		License			0		0								0
2.11.	HSM		Number	1		0		0								0
2.12.	Anti-Virus –malware and Anti-Spam (for Server & System administration OS)		Subscription/Year			0		0								0
Row Intentionally left Blank																
3.	**Backup Site 1/NLDC**															
3.1.	SAN (SAS based, 10TB usable capacity, expendable to 20TB usable)		Number	1		0		0								0
3.2.	UPS (To support above SAN, with 30 min power backup)		Number	1		0		0								0
Row Intentionally left Blank																
4.	**Lease line provisioning**															
4.1.	PDC to Backup Site 1/NLDC		Quarter	6		0		0								0
4.2.	PDC to NICNET Gateway 1		Quarter	6		0		0								0
Row Intentionally left Blank																
5.	**Data Center Rental costs**		Quarter	6		0		0								0
Row Intentionally left Blank																
	Total Cost (In Numbers) Including Taxes															*₹ 0*
	Total Cost (In Words) Including Taxes			***<<To be entered manually...>>***												

FORMAT 5B			Track 3: Phase 2 - Setting Up of PDC													
S No	Item	Open Source / Proprietary	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
	Hardware components															
1.1.	Blade Servers with 2X16 cores		Number	7		0		0								0
Row Intentionally left Blank																
	Supporting Platform															
2.1.	Operating system – Open source		Support			0		0								0
2.2.	Operating system - COTS		License/			0		0								0
2.3.	Virtualisation software		License/ CPU			0		0								0
Row Intentionally left Blank																
3.	**Core System Software Components**															
3.1.	Web server		Core	4		0		0								0
3.2.	Application Server		Core	4		0		0								0
3.3.	BPM Software		Core	4		0		0								0
3.4.	Document management system		Core	4		0		0								0
3.5.	Database – OIOS		Core	12		0		0								0
3.6.	Database security - OIOS		Core	12		0		0								0
3.7.	Database Administration Software Tool for DBA		User License	10		0		0								0
3.8.	GIS Server		Core	8		0		0								0
Row Intentionally left Blank																
	Total Cost (In Numbers) Including Taxes															*₹ 0*
	Total Cost (In Words) Including Taxes				***<<To be entered manually...>>***											

FORMAT 5C			Track 3: Phase 2 - Setting Up of DRC													
S No	Item	Open Source Proprietary /	Unit	Qty	Unit Rate	Total price (Excluding Taxes)	Tax %	Total price (Inclusive of Taxes)	Annual Technical Support (Inclusive of Taxes)							Total Cost of Ownership (Inclusive of Taxes)
									Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	
				A	B	C =AXB	D	E = C + (C*D/100)	Y1	Y2	Y3	Y4	Y5	Y6	Y7	F = E + Y1 + Y2 +Y3 + Y4 + Y5 + Y6 + Y7
			All Amount to be quoted in INR													
	Hardware components															
1.1.	Blade server chassis		Number	1		0.00		0.00								0
1.2.	Blade Servers with 2X16 cores (Total 128 Cores)		Number	4		0.00		0.00								0
1.3.	KVM Switch		Number	2		0.00		0.00								0
1.4.	SAN storage 40 TB Usable		License/ Support	1		0.00		0.00								0
1.5.	Racks		Number			0.00		0.00								0
1.6.	SAN Switch 24 Port		Number	2		0.00		0.00								0
1.7.	Access switch 10G		Number	4		0.00		0.00								0
1.8.	Structured Cabling within DC (Cat 6 A)		Job	1		0.00		0.00								0
Row Intentionally left Blank																
2.	**Security**															
2.1.	Firewall Next Generation with SSL VPN (1 GBPS cumulative throughput including 7.2, 7.3 and 7.4)		Number	2		0		0								0
2.2.	IPS		No	2		0		0								0
2.3.	Application Security		Subscription/Year	2		0		0								0
2.4.	URL filtering		Subscription/Year	2		0		0								0
2.5.	Anti-APT Solution with sand-boxing		Subscription/Year	1		0		0								0
2.6.	Web application firewall		No	2		0		0								0
2.7.	DLP (System administrators console)		License			0		0								0
2.8.	HIPS		License			0		0								0
2.9.	Privilege Management of System Administrator (VMs, Physical Servers, Storage)		LIC / VM			0		0								0
2.10.	Database Activity Monitoring		License			0		0								0
2.11.	HSM		Number	1		0		0								0
2.12.	Anti-Virus –malware and Anti-Spam (for Server & System administration OS)		Subscription/Year			0		0								0
Row Intentionally left Blank																
3.	**Core System Software Components**															
3.1.	Site Recovery Software		License/DR	1		0		0								0
3.2.	Web server		Core			0		0								0
3.3.	Application Server		Core			0		0								0
3.4.	BPM Software		Core			0		0								0
3.5.	Document management system		Core			0		0								0

3.6.	Database – OIOS		Core			0		0								0
3.7.	Database security - OIOS		Core			0		0								0
3.8.	Identity access and management		License			0		0								0
3.9.	GIS Server		Core			0		0								0
Row Intentionally left Blank																
4.	**Backup Site/NLDC**															
4.1.	SAN (SAS based, 10TB usable capacity, expendable to 20TB usable)		Number	2		0		0								0
4.2.	UPS (To support above SAN, with 30 min power backup)		Number	2		0		0								0
Row Intentionally left Blank																
5.	**Lease line provisioning**															
5.1.	Leased line between PDC, DRC of 50 Mbps		Quarter	6		0		0								0
5.2.	PDC to Backup Site 2/NLDC		Quarter	6		0		0								0
5.3.	DRC to NICNET Gateway 2		Quarter	6		0		0								0
Row Intentionally left Blank																
6.	**DRC Rental Costs**		Quarter	6		0		0								0
Row Intentionally left Blank																
	Total Cost (In Numbers) Including Taxes															*₹ 0*
	Total Cost (In Words) Including Taxes			***<<To be entered manually...>>***												

FORMAT 6		Centralized Helpdesk Resource				
S No	Resource Type	Indicative Person Months	Cost Per resource Per Month (Excluding Taxes)	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	C = A X B	D	E = C+(C*D/100)
1.	Application Support Manager	84		0		0
2.	Manager - L1 and L2	72		0		0
3.	Analyst - L1	168		0		0
4.	Analyst - L2	156		0		0
Row Intentionally left Blank						
	Total Cost (In Numbers) Including Taxes					₹ 0
	Total Cost (In Words) Including Taxes	*<<To be entered manually...>>*				

FORMAT 7		Training Cost (Inclusive of taxes)				
S No	Resource Type	Quantity/ Batch	Unit Cost Per training (Excluding Taxes)	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	C = A X B	D	E = C+(C*D/100)
All Amount to be quoted in INR						
1.	Agile Methodology Training	2		0		0
2.	Toolchain Training	2		0		0
3.	Training on the functional help desk tool	3		0		0
4.	Application Training Phase 1	21		0		0
5.	Application Training Phase 2	21		0		0
6.	OIOS System Admin Training	3		0		0
7.	Designing of MIS Reports/ dashboards	21		0		0
8.	UAT Training Phase 1	9		0		0
9.	UAT Training Phase 2	18		0		0
Row Intentionally left Blank						
	Total Cost (In Numbers) Including Taxes					₹ 0
	Total Cost (In Words) Including Taxes	***<<To be entered manually...>>***				

FORMAT 8		Track 6: Operation and Maintenance Cost											
S No	Resource Type	Qty	Cost / Resource / year	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Total Cost (Excluding Taxes)	Tax %	Total Cost of Ownership (Including Taxes)
		A	B	Y1	Y2	Y3	Y4	Y5	Y6	Y7	C = Y1+Y2+Y3+Y4+Y5+Y6+Y7	D	E = C+(C*D/100)
All Amount to be quoted in INR													
1.	**Operation & Maintenance**												
1.1	Operations Manager	1									0		0
1.2	Application Support Engineer	1									0		0
1.3	Developer/Sr. Developer	2									0		0
1.4	Tester	1									0		0
1.5	Database administrator	2									0		0
1.6	System Administrator	2									0		0
1.7	Infrastructure Manager	1									0		0
1.8	Analyst – BCP and DR	3									0		0
Row Intentionally left Blank													
2.	**Security Administration**												
2.1	Security Manager	1									0		0
2.2	Analyst (Application & Database Security)	3									0		0
Row Intentionally left Blank													
	Total Cost (In Numbers) Including Taxes												₹ 0
	Total Cost (In Words) Including Taxes	***<<To be entered manually...>>***											