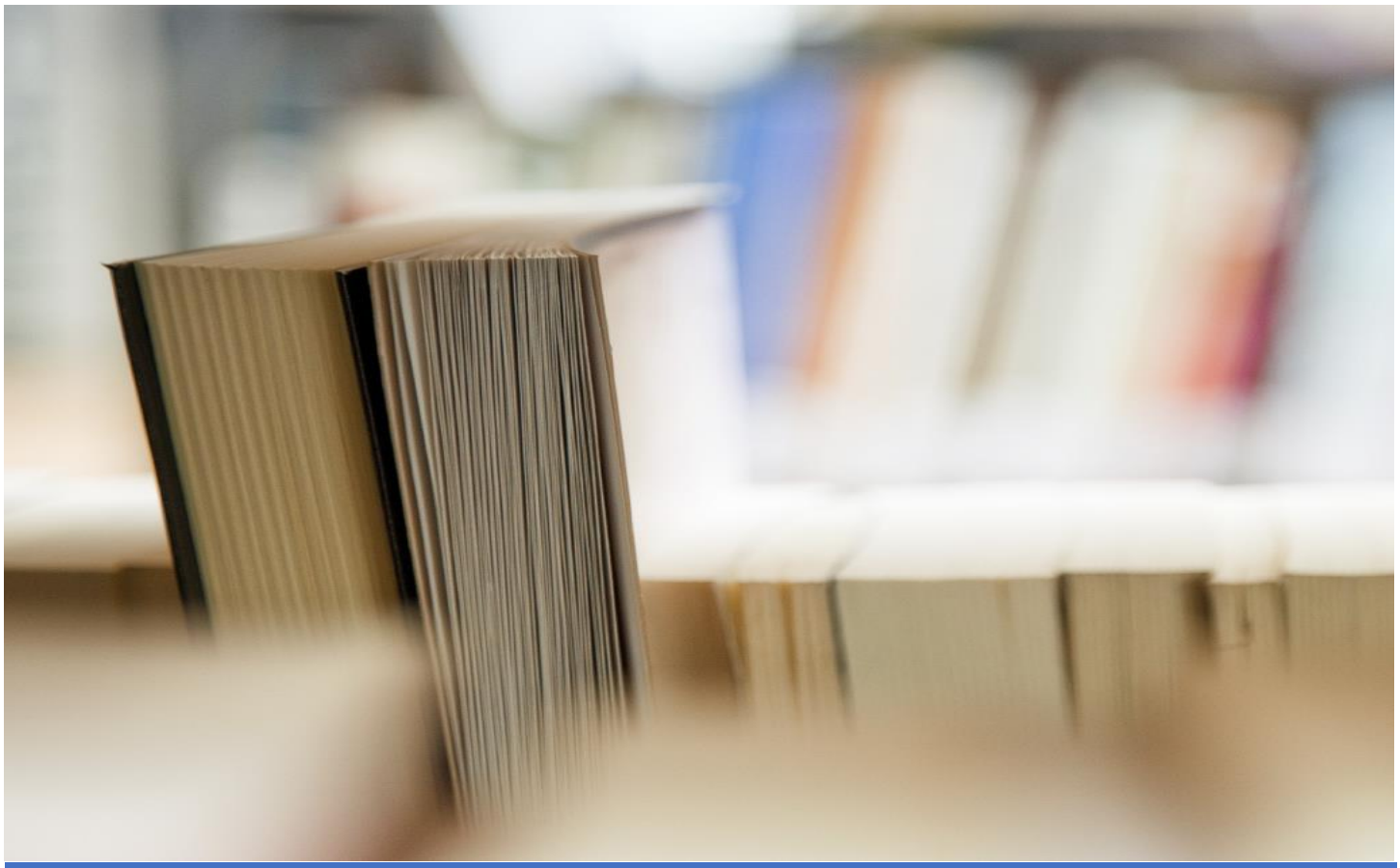


Specification Note for Internal Audit Management System for Internal Auditor of RGoB, Ministry of Finance, Bhutan

Table of Contents

1 Background

The Royal Government of Bhutan (RGoB) is pursuing reforms in Public Financial Management (PFM) through the PFM Multi Donor Fund administered by the World Bank. The reforms include strengthening the effectiveness of internal audit in RGoB and is intended to procure an Internal Audit Management System (IAMS) to enhance efficiency in the internal audit processes and reporting. Internal Audit in RGoB has progressed well over the past few years and further reforms are being pursued to replicate the best practices. The reforms are led by the Central Coordinating Agency (CCA) for Internal Audit Service under the Ministry of Finance supported by the 36 Internal Audit Units (IAUs) in Budgetary bodies. Human resources in internal audit are limited (there are a total of 45 auditors). Hence, it has been assessed that the use of Internal Audit Management System (IAMS) will build efficiency into the Internal Audit process and therefore maximize the effectiveness of the function.

CCA is looking for a comprehensive work-flow based Internal audit management solution which include at least the following modules; Audit Planning, Audit Scheduling, Audit Execution, Audit Reporting, Internal Audit (IA) performance tracking, Electronic Working Papers, Risk Management and Recommendation Tracking which is described succinctly in this document. The scope would include requisite training and implementation support. We are looking for a system to eliminate manual process in internal audit to improve productivity, bring a disciplined approach to the audit processes, track staff time on engagements, evaluate risks, improve reporting capabilities, and enhance follow up of audit recommendations. The IAMS can be COTS or BESPOKE solution.

2 Objective of Project:

The main purpose of this project is to develop an IAMS, capturing the entire internal auditing process beginning with audit planning to audit monitoring including follow-up and reporting.

3 Scope of IAMS:

3.1 The developer/vendorshall study the report on system architecture and functional requirement specification prepared by EY consultants (Appendix I) and develop/customize features in IAMS that are not covered by FRS under Appendix II, if it suits the needs of internal auditing process in RGoB IAS;

3.2 The developer/vendor shall seek technical design approval prior to the actual implementation of the project from the Department of Information Technology and Telecom (DITT), Ministry of Information and Communications;

3.3 The developer/vendor shall supply, design, develop/customize, install, testing, implement, In-build Audit Trail system and maintenance of a fully operational IAMS, based on the requirements stated in this tender document;

3.4 The developer/vendor shall ensure that IAMS integrate with other RGoB applications/systems with the capability of data extraction and analysis.

3.5 The Developer/vendor shall recommend the Hardware requirements for the IAMS system and provide price estimates for the hardware that are to be procured by CCA (infrastructure including licenses for all hardware, network, facilities, applications, and all other additional components necessary);

3.6 The Developer/vendor shall liaise and work with parties such as Data Center, telecom companies, Ministry of Information and Communication for hosting, facility management and any other relevant party appointed by Government;

3.7 The Developer/vendor shall provide maintenance and support services during the Launch, Warranty and Maintenance periods including a support structure to answer users' queries, problem escalation and processing of Service Requests;

3.8 The Developer/vendor shall ensure Internal Auditing Continuity with all the necessary services including backup and recovery processes/procedures;

3.9 Ensure that the system meets the security requirement as stated in this Tender Document

3.10 The developer/vendor shall provide a minimum of 10 minutes proposed IAMS System Demo;

3.11 The developer/vendor shall provide an updated User Manual and Technical Information throughout the duration of the Contract.

3.12 The developer/vendor shall provide user training to all the internal auditors and other ancillary activities as defined under Phase III, Section 9 (Deliverables and their schedule).

4 Internal Audit Management System (IAMS)

4.1 IAMS shall be a secured web-based system, serving all the internal auditors and head of government agencies.

5 Terminologies

For ease of reading, terminologies used in this document are:

Auditee:	Audit Client
CCA:	Central Coordinating Agency for Internal Audit Service
Consultant:	Consulting service provider for this task.
CoI:	Conflict of Interest
FAQ:	Frequently Asked Questions
IAMS:	Internal Audit Management System
IA:	Internal Auditor
IAU:	Internal Audit Unit
IA Plan:	Internal Audit Plan
MoF:	Ministry of Finance
PMO:	Prime Minister's Office

6 Proposed Strategy

6.1 The proposed IAMS strategy is to procure aIAMS solution and the CCA intends to procure/appointconsultant (Developer/Vendor) to deliver/develop/customize the solution and to maintain it for a period of one year.

6.2 IAMS will be hosted at a Government appointed Data Center and will use Government's SMS gateway but consultant must configure email service for notification.

6.3 To manage project complexity, IAMS will be implemented in three phases.

<table>
<tr><th>Phase I</th><th>Phase II</th><th>Phase III</th></tr>
<tr><td>Performance Security furnished.</td><td>Head of agency Homepage</td><td>Training</td></tr>
<tr><td>Contract agreement Signed</td><td>Approval of Internal audit Plan.</td><td rowspan="4">Propose training duration which should not exceed one week per batch comprising three batches of 15 staff each.</td></tr>
<tr><td>Work / delivery plan including Software architecture</td><td>Internal Audit Reports</td></tr>
<tr><td>IAMS Homepage</td><td>a) Assurance Report</td></tr>
<tr><td>Registration</td><td>b) Consulting Report</td></tr>
<tr><td>User's Homepage</td><td>Monitoring and follow-up</td><td rowspan="20">Prepare training contents and train internal auditors.</td></tr>
<tr><td>Supervisor Homepage</td><td>CCA Homepage</td></tr>
<tr><td>Internal Audit Annual Plan</td><td>Internal Audit Reports</td></tr>
<tr><td>Audit Engagement</td><td>Annual IAUs Plan</td></tr>
<tr><td>Internal Audit Report</td><td>a) Assurance Report</td></tr>
<tr><td>a) Assurance Report</td><td>b) Consulting Report</td></tr>
<tr><td>b) Consulting Report</td><td>Monitoring and follow up</td></tr>
<tr><td>Monitoring and follow-up</td><td></td></tr>
<tr><td>Internal Auditors' Homepage</td><td>PMO officials Homepage</td></tr>
<tr><td>Internal Audit Annual Plan</td><td>Internal Audit Reports</td></tr>
<tr><td>Audit Engagement</td><td>a) Assurance report</td></tr>
<tr><td>Internal Audit Reports:</td><td>b) Consulting Report</td></tr>
<tr><td>a) Assurance Report</td><td>Monitoring and follow-up</td></tr>
<tr><td>b) Consulting Report</td><td>Audit trail</td></tr>
<tr><td>Monitoring and follow-up</td><td>Testing and reporting on Phase II</td></tr>
<tr><td>Testing and reporting on Phase I</td><td></td></tr>
</table>

7 IAMS Cost Submission (Financial Proposal)

7.1 Consultants bidding for the project will have to quote for all Phases and by modules with maintenance cost of the project over the period of one year. The Developer must also quote for per man-day rate.

7.2 The consultant shall provide costing in accordance with financial proposal forms.Failure to quote accordingly may lead to disqualification.

7.3 The IAMS project will be evaluated based on the total cost of all the phases. However, the Government reserves the right to award IAMS to the same Developer in Phases/parts.

8 Sizing Information:

For the purpose of sizing for the project, the following are the estimated figures

No. IA Plan a year	: 50 Plans
Growth percentage per year	:2%
Average Size of each submission (in pages)	:30 pages
No. of Internal Auditing engagements	:500
Growth percentage per year	:10%
No of IAMS users (Internal Auditors)	:50
Growth percentage per year	:5%
No of IAMS users (IA Supervisor)	:50
Growth percentage per year	:2%
No of IAMS users (Head of agencies)	:50
No. of Internal Audit report	:500
Growth percentage per year	:10%
No of IAMS users (CCA officials)	:10
Average Size of each submission (in pages)	:30 pages
No. of Annual Internal Audit report	:1
Average Size of each submission (in pages)	:200 pages
No. of working papers	: 500
Growth percentage per year	:10%
Average Size of each submission (in pages)	:200 pages
No. of Internal Audit consulting report	:300 Reports
Average Size of each submission (in pages)	:30 pages
Growth percentage per year	:10%

9 Deliverables and their schedule:

9.1 The tentative timeline includes IAMS development/customization of all the phases and Implementation of system

9.2 The activities/deliverables of the assignment and Work Schedule are as tabulated below;

Phases	Deliverable	Expected Out come with milestones	Dateline.
Phases I	Signed Agreement	Contract agreement signed, Inception report submitted and accepted by client.	3rd December 2020.
	Performance Security		
	Inception report		
	Registration	Data base for users established with	18th March 2020

Phases	Deliverable	Expected Out come with milestones	Dateline.
	User's Homepage	user rights, Registration, user home page, supervisor home page developed, demonstrated and report approved by client (UAT signoff).	
	Supervisor Homepage		
	Internal Audit Annual Plan		
	Audit Engagement		
	Reports		
	Monitoring and follow-up		
	IA Homepage	IA home page and contents there in developed, demonstrated and report approved by client (UAT signoff).	
	Internal Audit Annual Plan		
	Audit Engagement		
	Reports		
	Monitoring and follow-up		
Phase II	Head of agency Homepage	Head of agency home page and contents therein developed, demonstrated and report approved by client (UAT signoff).	18th March 2021
	Approval of Internal Plan.		
	Reports		
	Monitoring and follow-up		
	CCA Homepage	CCA homepage and contents therein and PMO home page and contents there in developed, demonstrated and report approved by client (UAT signoff).	
	Reports		
	Monitoring and follow-up		
	Annual Internal Audit Report		
	PMO officials Homepage		
	Reports		
	Monitoring and follow-up		
	Audit trail		
Phase III	Prepare user manual on IAMS for different users	User manual printed out	18th May 2021
	Propose training duration which should not exceed one week per batch comprising three batches.	Final testing (UAT signoff).	
	Prepare training contents and course	Internal auditors trained on IAMS. and a training completion report submitted to client and approved.	
	Train (in class room with case studies) all the Internal Auditors on IAMS.		
	Prepare and submit project completion report	Project completion report submitted and approved by client.	

10 Other requirements;

a) Software architecture design document and customization methodology applied;

b) Application maintenance manual and data recovery manuals;

c) Source codes for customized solution, database scripts, and any relevant documentations to the management;
d) Monthly project status report (Status, issues)

11 Documentation

The Developer shall supply and deliver full documentation on all aspects of the System including but not limited to the following:

a) Project Plan including Risk Management and Schedule
b) Progress Reports
c) Technical Architecture Specifications with Asset lists/records
d) Functional Requirement Specifications which include items such as system overview, system environment, functional hierarchy, detailed functional requirements, interface requirements, system performance requirements, system security requirements, report formats and error messages exception handling.
e) Design Specifications, which include items such as application architecture, screen design /captures, navigation paths, report layouts, file layouts, system security design specifications, database architecture, data model, database schema, data dictionary, database design diagram, table and field definitions and description.
f) Installation and Implementation Plan
g) User Acceptance Test Plan, Package, Report
h) System Test Plan, Package, Report
i) Performance Test Plan and Report
j) Training Plan, Training Guide and materials
k) Configuration Management
l) Exit, Transition and Handover Plan
m) System Operation Manual, including system operation, database archival, configuration, database backup and recovery, etc.
n) Interface Design specifications which includes items such as data mapping and transformation specifications, data conversion, mapping test plans, test scenario and results
o) User Guide/User Operation Manual
p) Post Implementation Support Plan
q) Maintenance Plan
r) Transition / Exit Plan

The Developer shall maintain a copy of all the documentations and provide any other additional documentation as and when required during the contract period.

12 Responsibilities:

12.1 Procuring Agency (CCA):

12.1.1 Shall ensure once in every two weeks updates are reviewed and comprehensive requirement specifications are provided within review period;
12.1.1 Shall maintain the delay register and notify the Developer of all delays in writing;
12.1.1 Shall appoint the point of contact or project focal person(s);
12.1.1 Inform the stakeholders and arrange for joint sessions with developer;
12.1.1 Shall facilitate the developer/vendor in seeking technical design approval from the Department of Information Technology and Telecom (DITT), Ministry of Information and Communications prior to the actual implantation of the project.

12.2 Developer

12.2.1 Shall set up a dedicated development environment at developer premise with proposed team members working on the project.
12.2.2 Shall ensure timely delivery of deliverables;
12.2.3 Shall provide the IAMS development platform acceptable to client;
12.2.4 Shall maintain the delay register and inform the client on the delays;
12.2.5 Shall appoint a team leader who shall be the point of contact; and
12.2.6 Shall recommend and supply suitable infrastructure (server specifications and other necessary hardware) to host the IAMS safely and efficiently.
12.2.7 The developer/vendor shall seek technical design approval prior to the actual implementation of the project from the Department of Information Technology and Telecom (DITT), Ministry of Information and Communications.

13 Warranty (Phase wise)

13.1 IAMS warranty shall be quoted for every phase.
13.2 The Developer shall support during the Launch.
13.3 Provide one year of warranty after the user acceptance signoff. During this period, the Developer is responsible for technical support such as update patches; fix bugs, correct defects without any additional cost.
13.4 Make some minor changes such as changing of label names, adding simple labels on the page and tweaking color.
13.5 Tuning the application for performance and maintenance related activities whichincludes installation and configuration for a period of 12 months.

14 Ownership of Source Code

CCA shall be the owner of the source code for customized function of IAMS, Intellectual Properties and patent rights. Developer may propose their businessmodality of the ownership.

15 Maintenance and Support

15.1 The Developer shall provide comprehensive maintenance for all components propose.

15.2 Response time: Within two (2) hours from the time a service call is lodged.

15.3 The Developer shall provide IAMS Maintenance and Support Services that include the following:

a) Ensure and support the smooth running of the entire System.
b) Provide corrective maintenance, troubleshoot, and isolate software defects, including diagnosis and correction of all latent errors in the Application Software.
c) Provide interim solutions in the event while awaiting the corrective measures to correct any errors in the System.
d) Investigate and correct defects in the application system as reported by IAMS users within the service levels. The resolving effort includes resolving errors through developing, testing, and implementing changes to the System.
e) Fine-tune and improve the performance of the IAMS.
f) Manage, support, and implement, at the request of IAMS users, Service Requests, for the purpose of operational enhancements and IAMS upgrades.
g) Recover lost data, restore, and repair damaged data and correct erroneous data to the extent possible.
h) Assess impact of new releases, upgrades, or patches of IAMS and recommend updates or patches for production environment (eg: operating system and security patches).
i) Ensure that all modifications to the IAMS and Application software are properly integrated with the necessary components (hardware, software, firmware etc) and that the system performance is not degraded.
j) Provide solutions for problems encountered in the installation of all the software or both server and clients for the System to function properly.
k) Implement and operate a problem tracking system to log and track the progress of problem resolution.
l) Implement, at the request of IAMS users, software change requests, for the purpose of operational enhancements. The Developer shall prepare technical feasibility proposal including impact analysis for the IAMS change requests raised by the users.
m) Make modifications to the Application when requested and to perform system tests to ensure system integrity after modifications.
n) Ensure that all program source codes and executable codes are properly maintained (especially the versioning) and backed up.
o) Implement and enhance operational procedures as and when needed.
p) Produce ad-hoc reports when requested.
q) Produce and update technical and user documentation for the Application.
r) Monitor the Application to ensure data integrity and efficient performance and provide expert advice on applications performance monitoring and tuning.

s) Train personnel (with Administrator Role) on the software changes to enable them to be competent and self-reliant in the operation of the System.
t) Plan daily operations to ensure optimization of resources and batch windows utilization.
u) Schedule and ensure successful completion of ad hoc, daily, weekly, monthly and other batch processing jobs in the System.
v) Provide application systems support services, including technical advice and assistance to ensure continuity, availability, and accessibility of the System.
w) Ensure that the system operation is well protected in data security and disaster recovery.
x) Maintain all standards and procedures applicable to the System (e.g. generic modules or reusable component etc).
y) Work with Facility Management (FM) vendors and any other third parties to implement proposed procedures for back-up / recovery services, application deployment, system monitoring for the System.
z) Produce and update technical and user documentation on the System and Application Software.
    1. Attend to user queries and provide assistance to them in the operation of the System.
    2. Provide System briefings and support to users when needed.
    3. Provide advice, guidance, and training to CCA in the use of the System.
    4. Handle escalated Helpdesk calls where problem reported is related to the Application software and to work closely with Helpdesk to resolve all application systems problems within the service level.
    5. Assist Facilities Management Developer in the performance of software installation of the System and any new releases/upgrades.
    6. Prepare monthly progress and status report, supplementary documentation subject to review and approval by CCA.
    7. The Developer shall update CCA of all known software bugs and its problem resolution on a monthly basis or earlier if necessary.
    8. So long as the proposed software is in use by CCA, the Developer shall inform CCA, of any new releases of the application software, databases and development tools and provide information in the capabilities of the new version of the software and the impact analysis on the existing system.

16 Request Management

16.1 The Developer shall implement all Service Requests raised by CCAfor the purpose of System operational enhancements such as;
    1) Changes in business policy,

2) To support new functionality,
3) New business rules,
4) For System upgrades including hardware, software, and infrastructure services.
5) For each Service Request raised, the Developer's scope of work shall include the following but not limited to:
    a) Make an assessment on the Service Request and submit reports to CCA for written approval. The report shall detail the impact analysis and estimated effort required. This assessment and report will be considered as part of the operations support and therefore not chargeable;
    b) Carry out design, programming and testing work to modify the affected System in order to meet requirements of the Service Request. Where necessary, CCA reserves the right to request the Developer to re-test the affected System;
    c) Ensure all modifications to the System are properly integrated with the necessary components (hardware and/or software) and that the system performance is not degraded and to ensure system and data integrity are not compromised after modifications;
    d) Comply with the System Acceptance requirements;
    e) Handover to Operations with sufficient briefings and support; and
    f) Prepare / update all relevant technical, user or any other affected documentation to reflect changes made to the System.
    g) Maintain the records of Service Requests, its status and relevant documentations to be produced during audits.

16.2 The developer should make sure that the application developed in the system is as per Bhutan Government Internal Auditing standards.

17 Back-up and Recovery

17.1 The Developer shall in his proposal submit a backup and recovery strategy and methodology for the System. The methodology shall include hardware and software used, types of backup, frequencies of backup, as well as procedures for performing the backup and recovery.

17.2 The Developer shall add and quote for any additional backup software licenses required for future expansion of the proposed servers for the System.

17.3 The Developer shall note that the System recovery shall be within 24 hours when situations arise e.g system failure. "Data" is of utmost importance and there shall be "no loss" of data at any instance. The Developer shall work out a data backup plan (including backup and restoration procedures) for all software used in the System and test it to ensure data recoverability before the commissioning of the System. The Developer shall present the test plan/results to CCA for approval.

17.4 The detailed backup and recovery plan shall include the following areas:

a) Overview of backup and housekeeping strategy;
b) Time and resources required for backup for each of the transactions;
c) Detailed backup and recovery procedure;
d) Time and resources required for recovery for each of the transactions;
e) Data retention periods, frequency of backup, types of backup (such as incremental and full back up), the data to backup (such as application data files, system files);
f) Process of system recovery from the backups following a system failure; and
g) Roll-back procedures.

17.5 The data backup plan shall ensure that the backup and recovery process recover all transactions and data up to latest data backup transaction before the system failure occurred. The transaction and database logs of failure shall be backed up. As a general guideline to practice where operationally feasible:

a) Daily full data backup or incremental data backup shall be done on all systems for data protection and recoverability;
b) Minimally, weekly full backup must be done;
c) Minimally, six (6) generations of backup data shall be kept for the daily backup, recycled weekly;
d) Minimally, five (5) generations of backup data shall be kept for the weekly full backup, recycled monthly;
e) Minimally, twelve (12) generations of backup data shall be kept for the monthly full backup, recycled annually;
f) The latest backup shall be sent to government approved off-site storage on the following day for Disaster recovery. At any point in time, a full set of backup data i.e. full weekly backup plus daily incremental backup including the latest one, shall be stored at the off- site location for a full system recovery in time of need; and

g) Backup media lifespan must be tracked for prompt replacement of media to avoid loss of data.

17.6 The Developer shall ensure that the documentation remains up-to-date and all or any changes to the plan must be sent to CCA for approval at least one (1) month before the changes are to be executed.

17.7 The Developer shall perform daily data backup for the System, on-site and off-site media management, and data recovery activities.

17.8 The Developer shall perform quarterly data recoverability tests to ensure the recoverability of all data stored on the backup media.

17.9 The Developer shall keep an inventory list of all backup media and conduct 6-monthly inventory checks on the backup media to ensure their completeness, clear labeling and to housekeep the obsolete media. The Developer shall present the findings to CCA within 1 week upon the completion of check.

17.10 The Developer shall ensure that all manuals, documentation, and quality records for the System (e.g. forms) are being organized/filed in a well-structured manner and kept centrally. The Developer may on the request of CCA store the softcopy of the manuals, documentation and quality records at an off-site location identified by CCA.

17.11 The Developer shall ensure that the backup process/operation is not run during the CCA working hours in any month. If required to run during that period, it should not affect the system performance.

17.12 The Developer shall ensure that the System continues to operate during the period when back-up activities are running.

17.13 The System shall also provide for functions, which allows the System Administrator to perform database backup. The process of backup should be automated with user defined parameters.

17.14 The backup and recovery plan shall meet Disaster Recovery and Data storage requirements as specified in this section.

18 Problem Management

18.1 Service level;

18.1.1 The Developer shall ensure that all Helpdesk calls are attended to as per Service Levels defined below. Calls made outside operating hours should be routed to a voice mail and acted upon at the start of operation hours the next working day.

18.1.2 The problem resolution times shall depend on the severity level of the problem. The definition of the Business Impact /Severity Levels is as follows:

Business Impact/Service Level	Definition

Business Impact/Service Level	Definition
Severity 1	Defect that affects the System such that required operational objectives cannot be achieved, e.g. when a program crash or "hang" and the entire System has to be restarted.
Severity2	Defect that affects operational objectives and workaround is available. However, business can continue in a restricted manner.
Severity 3	Defect that affects a particular form of operation but does not affect any operational objectives as there may exist a temporary work around solution.

18.1.3 The call response time for ALL types/severity levels of problems shall be within two (2) hours of notification.

18.1.4 In addition to guidelines stated in the Conditions of System Maintenance and Support, the Service Level for Problem Analysis and Resolution shall be as follows:

Severity Level	Resolution Time	Frequency of Status Reporting
Severity 1	Within ONE (1) calendar day	Every 1/2 hour for problems that happens on the critical days of application peaks; otherwise, the frequency shall be every four (4) hours
Severity 2	Within THREE (3) calendar days	Daily
Severity 3	Within FIVE (5) calendar days; or within a period mutually agreed upon between the Developer and CCA	End of problem resolution

18.1.5 These Service Levels shall apply to the System during implementation, system warranty and maintenance period.

18.1.6 In the event of changes resulting from defective products, the Developer will be responsible for incorporating the changes at no cost to CCA. The Supplier shall be held solely liable for any time delay or damage, if such defects are not rectified. The Developer shall continue to work with the relevant parties to resolve the problem.

18.1.7 The Developer shall produce the consolidated report of all problems and show evidence that the overall response time and the other specified Service Levels are met. The report shall be submitted to CCA on a monthly basis or as and when requested by CCA.

18.1.8 For Severity 1 problems, the Developer shall provide in writing a preliminary report to explain the incident the following working day. Subsequently the Developer shall provide a post incident review report to explain in detail the cause of the incident,

the corrective actions taken and the solutions to prevent the incident from recurring, within five (5) working days after the incident has been rectified.

18.1.9 For Severity 2 and 3 problems, the post incident review reports shall be submitted within five (5) working days after the incident has been rectified.

18.1.10 The Developer shall note that the severity of a problem may be escalated based on circumstances such as high impact to user's operations.

18.1.11 The Developer shall provide a mechanism and substantiate to CCA that the Service Levels are met. There must be proper acknowledgement and monitoring of all reported defects and problems by the Developer.

18.1.12 The Developer shall be responsible to ensure that CCA Representative is kept updated on the latest status of the reported defects or problems without being prompted.

18.2 In the event of any dispute on the cause of the problem, the Developer shall demonstrate and prove why the element within the scope of this Contract and/or services rendered within the scope of this Contract is not the cause of the problem.

18.3 In the event the cause of the problem is traced back to the unsatisfactory resolution of the problem, the problem start date shall commence from the start date of the original "Problem Resolution Time".

18.4 The Developer shall schedule problem reviews to track unresolved problems and provide rectification efforts to prevent problem from reoccurring. Frequency of such reviews shall be specified by CCA.

18.5 CCA will review the form used by the Developer to capture the problem, and may propose its own form to use. This problem reporting form is to be submitted to CCA once a problem is reported.

18.6 The Developer shall perform a thorough analysis of the problem which includes identification of the cause of problem, the Systems affected, the data or any loss suffered and the recommendedsolution.

18.7 The Developer shall maintain a master list of all the problems, including at least the ticket number, the description of the problem, the caller, and the status, etc. CCA may request for this list at any point in time for review.

18.8 The Developer shall state the types and categories of change that are chargeable and indicate the cost involved.

18.9 The Developer shall take full ownership of all problems related to the availability of the System. In the case that the problem is traced to component(s) not supplied by the Developer, the Developer shall work with CCA to work with Bidders or procuring agencies to ensure that the problem is resolved, within the stipulated turnaround times.

18.10 The Developer shall have a mechanism to manage problem reporting of the System during the implementation, System Warranty and maintenance periods.

18.11 The Developer shall work with all parties designated by CCA and take whatever actions to resolve all problems and minimize system downtime.

18.12 The Developer is required to co-operate with third party vendors providing IT support services to CCA. If necessary, the System's operations management procedures will have to be refined by the Developer to accommodate the third-party systems.

18.13 The Developer shall make sure the third-party Developers' support personnel meets the corresponding service levels specified in, or are in accordance with, the current maintenance contract terms with the third-party Developers. The Developer shall obtain these service levels, as specified in the current maintenance contracts, for all the hardware and software from CCA.

18.14 It is the responsibility of the Developer to update and provide the updated copy of the Frequently Asked Questions (FAQs) and train the Developer's Helpdesk to support the System if the problem received necessitates such a change or update.

18.15 The Developer shall prepare and update all relevant technical, user or any other affected documentation to reflect changes made to the System. Updates in documentation shall be sent to CCA for review and approval.

18.16 A case is considered resolved when the reporting party is informed of the resolution by the Developer, but only closed upon successful completion and acceptance of User Acceptance Testing (if applicable).

19 Key Professional Staff

All experts who have a crucial role in implementing the contract are referred to as keyexperts. The profiles of the key experts for this contract are as follows:

19.1 Software Developer

Qualifications and skills

- Graduate in computer engineering/science/application or equivalent General

Professional experience

- Desired minimum of 5 years of experience
- Specific professional experience
- International experience with extensive hands-on experience in web technology and interoperability skills.
- Experience in programming in web services ajax, open architecture, writing source code, implementing solution to the assigned task.

19.2 System analyst

Qualifications and skills

- Graduate in computer engineering/computer science/ or equivalent
- General professional experience
- Desirable years of professional experiences-5years

- Specific professional experience
- Extensive hands-on experiences in system analysis, design, documentation.

19.3 Internal AuditExpert

Qualifications and skills

- CIA/CGAP/other professional Accounting certificationin addition to a University degree
- Fluency in English

General professional experience

- Minimum 10-year experience in Internal Auditing field covering the full audit life cycle

Specific professional experience

- Minimum of 5-year experience in Internal Auditing in government departments
- Must have international experiences
- Demonstrated experience of implementing and working on IAMS

20 Appendix I

Functional Requirement Specifications For IAMS Application For CCA and IAUs

provided by E&Y consultants

List of Abbreviations and Acronyms

Abbreviation	Full Form
AMS	Audit Management System
CCA	Central Coordinating Agency
CIA	Chief Internal Auditor
IA	Internal Auditor
IAU	Internal Audit Unit
IT	Information & Technology
MIS	Management Information System
PA	Performance Audit
RGoB	Royal Government of Bhutan
SMS	Short Message Service

1. Introduction

The detailed Functional Requirement Specification has been developed basis our report on "Report on Assistance in Identification and Selection of AMS/CAAT application "wherein the team had conducted the As-is study of the internal audit processes and study of CCA/IAUs requirements form the Audit Management System.

The objective of the assignment is to strengthen the internal audit of Royal Government of Bhutan. This is planned to be achieved by empowering staffs with latest skills, improved audit procedures and more efficient audit processes including use of IT tools.

The envisaged Audit Management System (AMS) will be a workflow-based web application with important functionalities like Audit Planning, Audit Execution, Audit Follow-up & Compliance, MIS Report etc. The envisaged Audit Management System (AMS) has been conceptualized to bring in transparency, efficiency and improve the monitoring of Audits in following ways:

- **Risk-Based Annual Audit Plan:** Execute risk profiling of audit units on the basis of available information of risk profiling parameters; selection of audit units on the basis of risk profiling result and prepare annual audit plan considering available human resource. Second tier transaction planning by integrating the AMS with external systems used by audit units.Automated intimation to audit units on list of documents required.Monitoring of performance of stakeholders by comparing achievement with planned target.
- **Monitoring & Control:**Automation of daily diary maintenance on the field and record the tour note of Internal Auditors for better monitoring of work on a day-to-day basis.
- **Reporting:** Automate preparation of audit reports in standardized formats, categorization of recorded paras, work-flow based review, approval and publication of audit reports.
- **Follow-up and Compliance:** System based automated follow-up mechanism and recording of compliance. Recording of audit para wise response received from concerned audit unit and dropping of paras.
- **Audit Management:** Allocate work and type of audit among team members of an audit party; Automate the preparation and submission of audit reports and manage the entire process effectively.
- **Efficient Para Management:** Manage audit paras effectively and improving the follow-up and supervision. AMS records the action required on the paras, designated officer responsible to prepare replies and timeline. It generates reminder emails and SMS for the concerned staffs to improve timeliness of replies.
- **Better communication and coordination:** Online management of paras will allow seamless communication among various officials at different levels. This will help the audit units to generate replies in electronic and print copies according to the required formats.
- **MIS report generation:** AMS expected to generate various customized monitoring reports required by RGoB. This portal will be helpful in creating such reports with minimal efforts.

1.1 Purpose

This document describes the functional requirements to design and develop the envisaged audit management System. This document covers the functional features of the application and non-functional characteristics of

the system like performance, security etc. This document is intended to serve as a guide to the developers (to know what to be developed?) and also as a software validation documents for the stakeholders.

1.2 Scope

The scope of this document includes the description of the proposed system covering the specific functional requirement specifications and non-functional requirements. Following critical processes have been covered under the purview of this project:

- Audit Planning
- Audit Execution & Reporting
- Follow-up & Compliance
- MIS Reporting
- Dashboard

1.3 Assumptions and Dependencies

The following assumptions have been considered while capturing the requirements

- The language used for the labels and reports in the system shall be available in English.
- Standard font used by RGoB will be used for both taking input and generating output in the system.
- The application is a web-based software which shall be accessible through a web browser.
- The web application will be hosted in Royal government of Bhutan owned Data Centre.
- The source code of the proposed application will be handed over to RGoB.

2. Functional Requirements

This section entails detail of module wise functional requirements identified during the course of study. This section covers following processes:

I. Functionalities to capture and maintain data

a. Audit Planning
   - Pre-Risk Assessment Configuration
   - Unit wise risk assessment data collection
   - Unit selection through Risk-Based Approach (Tier-1 Planning)
   - Detail Audit Planning: Annual Audit Calendar
   - Risk Profiling of Audit Processes
   - Unit wise Transaction Sampling (Tier-2 Planning)
   - Intimation to audit units

b. Audit Execution & Reporting
   - Entry conference
   - Daily diary maintenance
   - Draft audit observations recording
   - Exit conference
   - Release of draft audit report to audit unit
   - Record management response
   - Finalization of audit report

c. Follow-up & Compliance
   - Submission of Action Plan by Audit Unit
   - Intimation to audit units on pending compliance
   - Recording of audit observations wise compliance

d. MIS Reporting
   - Consolidation of Audit Observation by IAUs
   - Submission of Consolidated Report to CCA
   - Generation of IAU/ Unit wise Performance & MIS Reports

e. Master Data Management
   - Audit Unit Master
   - Auditor Master
   - Audit Party Master
   - IAU Master
   - Ministry Master
   - Autonomous Body Master
   - Dzongkhags Master
   - Audit Risk Parameter Master (both for Internal / Performance Audit) with broad category (i.e. all the risk parameters will be broadly classified into five broad categories i.e. Financial Risk, Technical Risk, Environmental Risk, Political Risk and Social Risk)
   - Audit Para Type Master
   - Audit Para Risk Priority Master
   - Audit Unit Type
   - Audit Unit Type wise Man-days

- Process/Internal Control Master
- Audit Documents Master
- External Integration Configuration

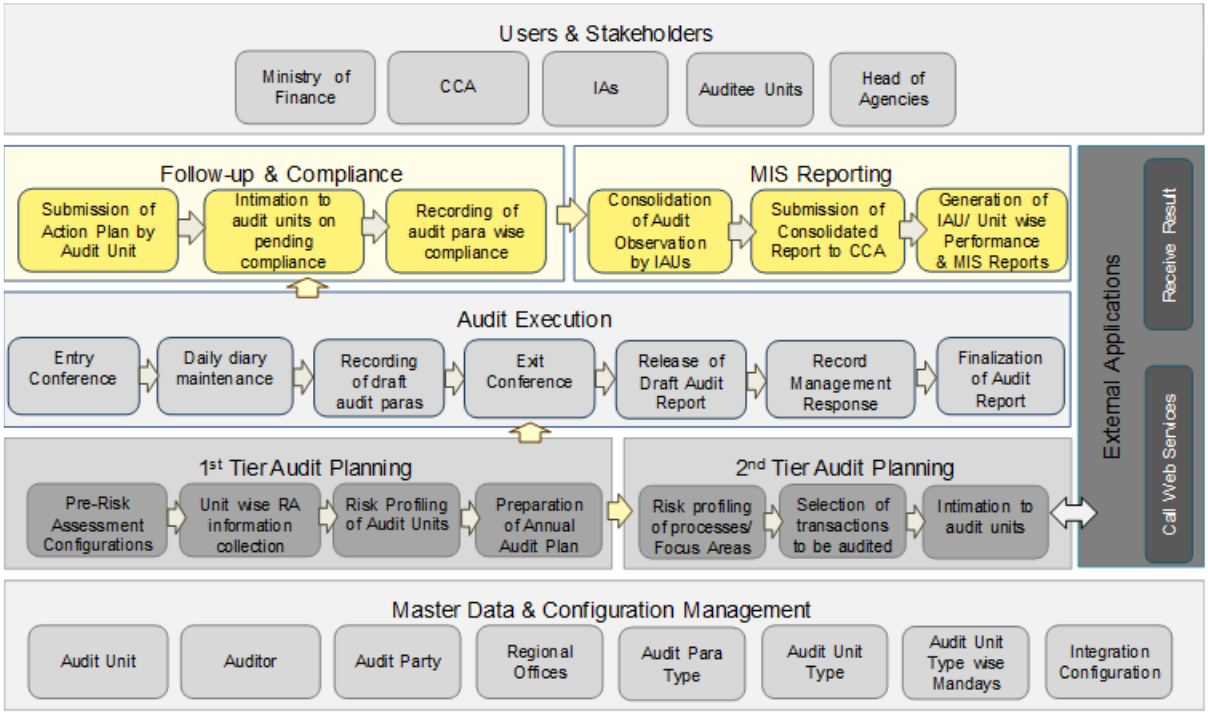
f. User Management

- User List
- Role Master
- Create New user
- Grant Privileges
- Change Password

II. *Functionalities to integrate IAMS with other applications with* the capability of data extraction and analysis.

III. Dashboards

- CCA Dashboard
- Finance Ministry Dashboard



- IAUs Dashboard
- Auditee Units Dashboard
- Common User Profile

Figure: Functional Architecture of Audit Management System

Functional Architecture

A Functional Architecture is an architectural model that identifies system functions and their interactions. It defines how the functions will operate together to perform the system mission(s). The functional architecture of AMS is being divided into eight sections, each with list of its own objective. In order to support the functional

development of AMS application, along with the verification tasks that are defined to verify the functional, performance and constraint requirements following architecture diagram is created.

2.1 Audit Planning

2.1.1 Process Definitions

Process Definition: Pre-Risk Assessment Configuration

Sl.	Steps	Actor/ Competent Authority
1	Internal Auditor at IAU will prepare and verify the list of audit units, makes required addition/ deletion to update the audit unit list.	IA at IAU
2	Chief Internal Auditor at IAU views the list of audit units and take required action (Approve/ Reject). If there is no CIA at IAU then IA will self-approve the same. Please note that If rejected, the system will send back to Internal Auditor at IAU for revision. And IA will revise accordingly and resubmit for approval.	CIA/IA at IAU
3	Internal Auditor at IAU will select the audit type (for e.g. performance audit/internal audit) wise required risk assessment parameters from available list for a particular year and send for approval. Internal Auditor at IAU may also add the additional parameters specific to the respective government agency pertaining to Internal Audit / Performance Audit. (Note 1: There will be some risk parameters which will be common for all the IAUs and some risk parameters specific to respective IAUs. There will be mapping of risk parameters to respective IAU.) (Note 2: All the risk parameters will be broadly classified into five broad categories i.e. Financial Risk, Technical Risk, Environmental Risk, Political Risk and Social Risk)	IA at IAU
4	IA/CIA of CCA views the submitted list of risk assessment parameters (for newly added only) and take required action (Approve/ Reject). Please note that If rejected, the system will send back to Internal Auditor at IAU for revision. And IA will revise accordingly and resubmit for approval.	IA/CIA of CCA
5	IA at IAU will assign weightage against audit type wise (for e.g. performance audit/internal audit) each risk assessment parameter and submit for approval. Basis IA of IAU risk assessment, same risk parameter can have different weightage for different IAUs.	IA at IAU
6	CIA at IAU views the submitted list of risk assessment parameters wise weightage and take required action (Approve/ Reject). If there is no CIA in IAU then IA will self-approve the same. Please note that If rejected, the system will send back to Internal Auditor at IAU for revision. And IA will revise accordingly and resubmit for approval.	CIA/ IA at IAU
7	Internal Auditor at IAU can define/ modify evaluation criteria. against	IA at CCA

Sl.	Steps	Actor/ Competent Authority
	each risk assessment parameter and submit for approval. Same risk parameter can have different evaluation criteria for different type of IAUs (i.e. IAU at Ministry/ Autonomous Body and Dzongkhags/Local Government)	
8	CIA of CCA views the submitted list of risk assessment parameters wise evaluation criteria and take required action (Approve/ Reject). Please note that If rejected, the system will send back to Internal Auditor at IAU for revision. And IA will revise accordingly and resubmit for approval.	CIA of CCA

Process Definition: Preparation and Approval of Annual Audit Plan (Tier 1 - Planning)

Sl.	Steps	Actor/ Competent Authority
1	IA/CIA of IAU will create Audit Parties and system will map available internal auditors to Audit party as Members/ Leader. Mapping of auditors to audit parties will be done by the system on random basis. Chief Internal Auditor/ Internal Auditor at IAU can also create audit parties manually.	CIA/ IA at IAU
2	System automatically calculates the number of available man-days on the basis of created audit parties and available working days.	System
3	IA/CIA of IAU selects a type of audit, type of audit unit and planning year. The system will automatically populate the list of available audit units.	IA/ CIA at IAU
4	The system will allow the IA/CIA of IAU to retrieve unit wise,audit type wise values of various risk assessment parameters from both AMS database and external systems through integrated web-services. List of sample parameters is as follows: Financial Risk parameters of Internal audit: • Total Budgeted expenditure in the previous financial year • Total fund received during the previous financial year	
5	The system will also allow entering/ importing unit wise risk assessment parameter details manually in case there is any problem in retrieving the same from external system.	
6	System will automatically populate unit wise values of other risk-assessment parameters (Arrears in audit/ Pending audit observations) from the AMS internal database.	System
7	Chief Internal Auditor/ Internal Auditor at IAU will execute the risk assessment of all units through system. On execution of risk assessment, the system willcategorise the audit units into (critical/high/medium/low) on the basis of allotted risk ranking in the master configuration.	IA/ CIA at IAU
8	The system will help the Chief Internal Auditor/ Internal Auditor at	System

Sl.	Steps	Actor/ Competent Authority
	IAU in selection of audit units on the basis of allotted risk rank (critical/high/medium/low). The selection criteria of the audit units will be prescribed by the respective IAUs. For example: - ► Select all the audit units having risk rank as critical for audit during year ► Select 50% of audit units having risk rank as high for audit during year ► Select 30% of audit units having risk rank as medium for audit during year ► Select 10% of audit units having risk rank as low for audit during year	IA/ CIA at IAU
9	The system prepares a draft audit plan by assigning available audit party to audit units on the basis of risk-rank of audit units.Date of audit will be calculated automatically by the system. (please note that IAs at IAU can also modify the plan based on the available man days with proper justification. There may be the possibility that system through a plan for example to audit 30 audit units (combination of critical risk, high risk, medium risk, low risk audit unit) but auditor is only having available man days for 20 audit units. Then it will on the desecration of the Internal Auditor to select which 20 he/she can audit with proper justification). The system will create a database wherein which of the audit selected by the system for planning but could not be audited by internal auditor due to less no. of available man days) The system will also give vice versa option, wherein the plan as per the system is less than the no. of audit unit can be audited by the Internal Auditor with available man days.	System IA/ CIA at IAU
10	Chief Internal Auditor/ Internal Auditor at IAU makes required changes in the audit plan and submits for approval to Secretary/head of respective government agency.	IA/ CIA at IAU
11	Secretary/head of respective government agencywill view the draft audit plan submitted and take required action (approve/ return). If returned, the system will send the draft audit plan to Chief Internal Auditor/ Internal Auditor at IAU for revision. Please note that as a practice to maintain the Internal Auditor Independence, the Secretary/head of respective government agency cannot reject the overall annual audit plan. However, can suggest addition audit unit to be audited in that year.	Secretary/head of respective government agency
12	On Approval of audit plan, audit units and audit parties will be intimated through auto generated SMS/ Email about audit calendar two weeks before the start of the audit. This letter also includea unit-wise list of documents required for audit (books of accounts, financial statements, registers, etc.).	System
13	The post structure and approver hierarchy in the system should be	System

Sl.	Steps	Actor/ Competent Authority
	dynamic and configurable. System should allow system administrator to do required configuration as and when required.	Administrator

Process Definition: Audit unit wise transaction sampling (Tier 2 - Planning)

<table>
<tr><th>Sl.</th><th>STEP</th><th>ACTOR/ COMPETENT AUTHORITY</th></tr>
<tr><td>1</td><td>The IA/CIA of IAUswill fetch the list of transactions of audit units (if available in the IT system integrated with the AMS for example MYRB/EPEMS used by audit units). This will allow the audit team to do second tier risk-based analysis.</td><td>IA/ CIA at IAUs</td></tr>
<tr><td>2</td><td>The system will allow the user to view and analyse the transactionsofdifferent processes like procurement, schemes, program expenses, office expenses, Assets and cash & bank. These processes will be mapped to type of audit.
The system will allow analysing risk rank of processes through a risk assessment check list mechanically. User need to select a type of audit and process to get the check list.
The system will be finding out the risky transactions from available list on the basis of percentage of value and number of transactions.
The system will not allow the user to make any change in the list of suggested risky transactions.
<table><tr><th rowspan="2">Risk Category of unit (Tier I)</th><th colspan="2">Procurement</th><th colspan="2">Own Source Revenue</th><th colspan="2">Financial Management</th><th colspan="2">Cash and Bank</th></tr><tr><th>Coverage in Amount</th><th>Coverage in Number</th><th>Coverage in Amount</th><th>Coverage in Number</th><th>Coverage in Amount</th><th>Coverage in Number</th><th>Coverage in Amount</th><th>Coverage in Number</th></tr><tr><td>High</td><td>80%</td><td>40%</td><td>80%</td><td>40%</td><td>80%</td><td>40%</td><td>80%</td><td>40%</td></tr><tr><td>Medium</td><td>60%</td><td>30%</td><td>60%</td><td>30%</td><td>60%</td><td>30%</td><td>60%</td><td>30%</td></tr><tr><td>Low</td><td>40%</td><td>20%</td><td>40%</td><td>20%</td><td>40%</td><td>20%</td><td>40%</td><td>20%</td></tr></table>For example, for a high-risk audit unit the system will fetch the list of transactions those are covering at-least 80% of total value and 40% of number of transactions (Refer above table) as risky transactions.
Note: The system will analyse and show risky transactions selected using both the approach (random and high value first).
Audit Management System should not provide facility to the auditors to make changes in the list of transactions suggested by the system. The list of suggested transactions should be locked for any change.
In case integration of sub-systems used by audit unit is not possible the risk assessment of processes and transactions will be done manually. In such cases the system will provide separate page to capture the outcome of manually executed 2nd tier risk assessment (risk rank of processes and list of process wise risky transactions).
For the purpose of performance audit, the internal auditor will evaluate in detail, the risk prevailing at the selected audit unit for the topic/program/theme selected for audit and choose the focus area.</td><td>Internal auditor at IAUs</td></tr>
</table>

Sl.	STEP	ACTOR/ COMPETENT AUTHORITY
	Accordingly, will select the extent of audit required whether the audit to be done all the sub division level of that audit unit or sample of audit unit for the topic/program/theme selected for audit. The user can also perform the evaluation of audit for topic manually and the system will have option to capture the results.	
3	Internal Auditor at IAU can view and download/ take print out of list of process wise risky transactions.	Internal Auditor at IAU
4	The system will allow configuration of risk category wise Coverage in Amount and Coverage in number of transaction.	Administrator

Process Definition: Intimation to Audit Units

Sl.	Step	Actor/ Competent Authority
1	The system will allow configuration of Message/ Email content.	Administrator
2	The System will allow configuration of advance time period (e.g. one/two week) during which auto-generated email/ SMS will be sent.	Administrator
3	The system will send intimation to audit units on audit calendar and required documents through auto generated SMS and email two week before the start of the audit.	System
4	The system will allow Internal Auditor at IAU to send reminder to selected audit units on any date prior to audit execution.	Internal Auditor at IAU

2.1.2 Functional Requirement Specification

FRS Sr. No.	Sub-Module	Requirement Description
FRS_AUPL_001	Access of online system	▶ System will allow the following role-based access to the authorized users: ● Internal Auditor at IAU: finalizing audit units database, finalize risk assessment parameters, assign weightage and evaluation criteria, configure risk rank configuration, perform risk-assessment, prepare and submit draft audit plan. ● CIA at IAU: Approve/ Reject draft list of audit units, Approve/ Reject ● Secretary/head of respective government agency: view/ approve/ return for revision of audit plan ● CIA/IAU of CCA: Approve/Reject the risk assessment parameters, Approve/Reject the evaluation criteria of Risk Assessment Parameter. ● Audit Unit in-charge: get auto generated system

FRS Sr. No.	Sub-Module	Requirement Description
		notification on audit calendar, list of documents etc.
FRS_AUPL_002	Pre-risk assessment configurations	▶ The system will allow Chief Internal Auditor / Internal Auditor at IAU to finalize the list of audit units before initiating the audit plan of a particular year.
FRS_AUPL_003	Pre-risk assessment configurations	▶ The system will allow Internal Auditor at IAU to assign the risk assessment parameters and send them for approval to CIA of CCA. ▶ The system will allow Internal Auditor at IAU to assign weightage and send them for approval to CIA of IAU (If there is no CIA in IAU then IA will self-approve the same) ▶ Chief Internal Auditor / Internal Auditor at IAU can define and approve evaluation criteria before initiating the audit plan of a particular year.
FRS_AUPL_004	Initiate audit plan	▶ The system will allow Chief Internal Auditor / Internal Auditor at IAU to initiate the audit planning process.
FRS_AUPL_005	Initiate audit plan	▶ The system will allow updating required information (audit parties, available party days and audit units with pending years) are up to date in AMS.
FRS_AUPL_006	Risk Profiling of Audit Units	▶ The system will provide facility to automatically retrieve audit unit wise risk assessment parameters from integrated external system and internal AMS database.
FRS_AUPL_007	Risk Profiling of Audit Units	▶ The system will allow defining new risk assessment parameters in the system and configure the data retrieval policy (web service/ internal database).
FRS_AUPL_008	Risk Profiling of Audit Units	▶ The system will also provide facility to record audit unit wise value of risk assessment parameters at different level (IAU/ Audit Unit) manually (In case data is not retrievable from external system).
FRS_AUPL_009	Risk Profiling of Audit Units	▶ The system will allow the Chief Internal Auditor / Internal Auditor at IAU of to perform risk profiling of audit units on the basis of defined risk assessment parameters.
FRS_AUPL_010	Prepare new audit plan	▶ The system will allow creation of new audit parties in the system by selecting available auditors from available list.
FRS_AUPL_011	Prepare new audit plan	▶ The system will allow creating duty calendar of each auditor considering available holidays in government calendar.
FRS_AUPL_012	Prepare new audit plan	▶ The system will allow populating list of available audit units and entering audit unit wise pending audit years.
FRS_AUPL_013	Prepare new audit plan	▶ The system will allow preparing new audit plan by Chief Internal Auditor / Internal Auditor of IAU.
FRS_AUPL_014	Prepare new audit plan	▶ The System will allow selecting audit unit from available list by filtering them with risk profile, unit type and locality wise.
FRS_AUPL_015	Prepare new audit plan	▶ The system will allow mapping of auditors to audit units. The system will assist the user by suggesting tentative audit calendar (audit unit, audit party, audit schedule) on the basis of audit unit type wise no. of days required, available working days and

FRS Sr. No.	Sub-Module	Requirement Description
		available auditors. ► Chief Internal Auditor / Internal Auditor at IAU can define/ modify audit unit type wise time required for internal audit and other audits.
FRS_AUPL_016	Prepare new audit plan	► The system will allow updating/ deleting existing audit plans by Chief Internal Auditor / Internal Auditor at IAU.
FRS_AUPL_017	Prepare new audit plan	► The system will restrict deleting of existing audit plan if it is already approved. However, users can modify the audit plan according to available man days and add additional units for audit as suggested by their secretary / head of agency.
FRS_AUPL_018	Prepare new audit plan	► The system will allow modification in audit party composition as and when required with specific reason like leave/ absence.
FRS_AUPL_019	Approval of audit plan	► The system will allow Chief Internal Auditor / Internal Auditor at IAU to submit the final audit plan for approval to secretary/ head of respective government agency.
FRS_AUPL_020	Approval of audit plan	► The system will allow secretary/ head of respective government agencyto approve the audit plan or return for revision with remark.
FRS_AUPL_021	Modify audit plan	► The system will allow Internal Auditor to make required changes in the existing audit plan (only addition of additional audit units) as per the feedback of secretary/ head of respective government agencyand re-submit for approval.
FRS_AUPL_022	Intimation of final audit plan to ROs	► On approval of final audit plan the same will be intimated to audit unit offices.
FRS_AUPL_023	General	► On saving the final consolidated audit plan IAU the record will be assigned with a unique plan id as follows: <YEAR>+<IAU_CODE>+<PLAN_SL>
FRS_AUPL_024	Quarterly/ Monthly Plan	► The system will allow viewing of quarterly/ monthly detailed audit plan.
FRS_AUPL_025	Second tier Planning	► The system will provide Internal Auditors to retrieve transactions of specific audit units from external IT systems (i.e. MYRB/EPEMS) used by concerned audit unit (if AMS is integrated with external IT systems used by concerned audit unit).
FRS_AUPL_026	Second tier Planning	► The system will provide Internal Auditors to analyse retrieved the transactions and generate list of risky transactions, heads, items, vendors etc.
FRS_AUPL_027	Retrieve information	► System will allow retrieving annual audit plan information after entering year, IAU, plan no, audit type, unit type, unit name etc.
FRS_AUPL_028	System functionalities	► System will retain the saved information in case of any error or abrupt closing of current page.
FRS_AUPL_029	Reports	► The system will allow the users to print and download the annual audit plan.
FRS_AUPL_030	Reports	► System will allow to generate the reports based on certain pre-defined parameters.

FRS Sr. No.	Sub-Module	Requirement Description
FRS_AUPL_031	System functionalities	▶ System will have data entry module for master data entry with roles for information creator and verifier.
FRS_AUPL_032	System notifications	▶ The system will display appropriate messages like: ▶ Confirmation message: Unique Plan id generated; Plan details updated; Email/ SMS notification sent etc. ▶ Error message in case of unsuccessful transmission: Plan id cannot be edited; etc. ▶ Messages pertaining to role based access controls will also be displayed like: You are not authorized to perform this action etc.

2.2 Audit Execution and Reporting

2.2.1 Process Definition

Process Definition: Entry Conference

Sl.	Step	Actor/ Competent Authority
1	IA/CIA of IAU will record the details of entry/ opening meeting with audit unit. Following information are recorded in the system: a. Name of the Audit Unit b. Audit Year c. Meeting Date d. Members Present (Name, Designation, email id) e. Points Discussed f. Attachment if any	IA/ CIA of IAU
2	Information recorded by Internal Auditor is submitted to CIA of IAU for approval. If there is no CIA at IAU then approval not required.	CIA of IAU
3	CIA of IAU views the submitted information and take necessary action (Approve/ Reject with Remark). Please note that If rejected, the system will send back to Internal Auditor at IAU for revision. IA will revise accordingly and resubmit for approval.	CIA of IAU
4	Once the Opening Meeting is recorded then system will allow recording of information related to internal auditors joining/ leaving audit party. Information like Date, Time (AN/ FN), Name of the Auditor/ Audit Personnel, Name of the Audit Unit, Start Date, End Date, Reason (If Any) will be recorded in the system.	CIA/ IA of IAU

Process Definition: Work Allocation

Sl.	Step	Actor/ Competent Authority
1	The Chief Internal Auditor of IAU select a team member from available list and allocate specific work to the team member / other Internal Auditor of IAU through the system. Note: List of work to be allocated to team members / other Internal Auditor of IAU can be configured in the system which includes list of documents, registers, books of accounts, list of procurement, etc. Chief Internal Auditor of IAU does the work allocation among team members / other Internal Auditor of IAUand record the same in the system. Following information are recorded in the system: a. Name of the Audit Unit b. Audit Year c. Review Period	CIA of IAU

Sl.	Step	Actor/ Competent Authority
	d. Audit Party e. Date f. Name of the Audit Party Members/ Auditor g. Type of Audit (Internal Audit/ Performance Audit) h. Work Assigned i. From Date Time j. To Date Time k. Remark if any If there is only one Internal Auditor as audit party team then the member can assign work to him/ her self.	
2	The captured details will be visible to the Chief Internal Auditor of IAU for confirmation/ approval. Once it is approved the record will be locked for any modification.	CIA of IAU

Process Definition: Execution Checklist

Sl.	Step	Actor/ Competent Authority
1	Internal Auditor of IAU conduct auditand record audit paras in the system and submit it to CIA of IAU for verification. If no CIA at IAU then verified by Himself/herself. The system will also allow performing audit and testing of internal controls of audit units. In case of Internal / performance audit and testing of internal control the system will allow the internal auditor to evaluate audit organisations through pre-defined checklists. These checklists (parameters, allowed value/ value-sets) can be configured in the system. Discrepancies recorded against parameters will generate audit paras. The system will provide facility to record observation of auditors through audit execution checklist. The customized checklist depends upon the type of audit can be configured in the system. For example, the performance audit is to be performed for topic/theme/program/scheme and hence for every such type of topic/theme/program/scheme a specific checklist will be required to execute the audit. Hence, internal auditor will prepare these specific checklists based on his professional judgement and upload it into the system.	CIA/IA at IAU
2	User will select a process/ area from available list. System will fetch a list of available sub-process/ sub-area (if any) under the selected process.	CIA/IA at IAU
3	The system will then populate the list of questions relevant to the	CIA/IA at IAU

Sl.	Step	Actor/ Competent Authority
	type of audit.	
4	User need to select response (Yes/ No/ N/A) against each question and save.	
5	User can create audit memo/observation against each question answered as no.	
6	User can also create audit memos/observation directly in the system for a selected audit unit for a specific review period.	
7	User need to capture following information while creating a memo/audit observation: a. Audit Unit b. Type of Audit c. Audit Year d. Review Period e. Memo/Audit observation Date (Auto from session) f. Memo/ Audit observation Number (Auto) g. Memo/ Audit observation Type h. Amount Involved (if in question) i. Observation Type j. Audit Process, Head k. Memo/ Audit observation title l. Audit observation Description - the audit observation description will be further sub categorised into ▸ Condition ▸ Criteria ▸ Causes ▸ Consequences/Effect/Impact m. Attachment if any	CIA/IA at IAU
8	Internal Auditors of IAU submits the created memo/audit observation for approval to audit CIA at IAU. If no CIA at IAU then self-approval by IA of IAU.	CIA/IA at IAU
9	CIA at IAU will review the memo/audit observation and take necessary action (approve/reject with remark). If no CIA at IAU then self-approval by IA of IAU.	CIA/IA at IAU
10	Once the Audit Memo/audit observation is approved by the CIA of IAU it will be sent automatically to audit unit for response.	CIA at IAU/ System
11	After receiving the memo/audit observation from CIA/IA of IAU the audit unit submits response against it.	CIA/IA of IAU
12	User will be able to see list of audit memos/observations created by him and his team member.	CIA/IA of IAU

Sl.	Step	Actor/ Competent Authority
13	After receiving response from audit unit, the Internal Auditor decides whether the memo/observation need to be dropped or to be converted to audit para. If the audit para is dropped by the Internal Auditor, then the status of the memo/observation will be changed to DROPPED. If the memo/observation is converted to para then the status will be changed to CONVERTED_TO_PARA. Any memo/observation can be converted to para at any point of time. If response is not received on time, then also a memo/observation is automatically converted to para updating its status to CONVERTED_TO_PARA. Following information will be recorded while creating a para: a. Audit Unit b. Type of Audit c. Audit Year d. Review Period e. Audit Party f. Auditor g. Observation Type h. Audit Process, Head i. Observation Type j. Amount Involved k. Amount Recoverable l. Para Category (Auto) m. Para Risk Priority n. Para Title n. Detail Description of Para - the audit observation description will be further sub categorised into ▶ Condition ▶ Criteria ▶ Causes ▶ Consequences/Effect/Impact ▶ Recommendation o. Attachments p. Related Section q. Concerned Official (Name, Designation, email id) r. Timeline System will also provide facility to define observation type wise input parameters dynamically against which the auditor will capture data. Such configurations will be done by the administrator only. While	CIA/IA of IAU

Sl.	Step	Actor/ Competent Authority
	defining a parameter user will mention details like Label, Input Type (Text/ List/ Checkbox/ Option), Data Source/ Fixed Data List, Is Compulsory, Help Text, Validation etc.	

Process Definition: Convert Audit Memo to Para

Sl.	Step	Actor/ Competent Authority
1	Once the audit para is created then the same will be submitted by the Internal auditor to CIA of IAU.	IA of IAU
2	CIA of IAU can either approve the audit para or return with remark to the creator.	CIA of IAU
3	If the audit Para is approved by the CIA of IAU then it will be included in the draft audit report.	IA/ CIA of IAU

Process Definition: Daily Diary Maintenance

Sl.	Step	Actor/ Competent Authority
1	Internal Auditors take entry in online daily diary at every day-end on the basis of activities performed against assigned work.	IA of IAU
2	Acknowledgement of online daily diary entries by CIA of IAU.	CIA of IAU

Process Definition: Exit Meeting

Sl.	Step	Actor/ Competent Authority
1	IA/ CIA of IAU will record the details of exit/ closing meeting. Following information are recorded in the system: a. Name of the Audit Unit b. Audit Year c. Meeting Date d. Members Present (Name, Designation, email id) e. Points Discussed f. Attachment if any	CIA/IA of IAU
2	Information recorded is submitted to CIA of IAU for approval. If no CIA at IAU it will be self-approved by IA himself/herself.	IA/CIA of IAU
3	CIA of IAU views the submitted information and take necessary action (Approve/ Return with Remark).	CIA of IAU
4	Once the Closing Meeting is recorded then system will not allow recording of daily diary details.	System

Process Definition: Audit Report (Preparation/ Review/ Approval)

Sl.	Step	Actor/ Competent Authority
1	IA of IAU will select an audit unit and review period for recording following details to complete preparation of draft audit report: a. Auditee Details b. List of Officials met c. Audit party details d. Audit details (Scope and Coverage) e. Audit Para type f. Audit para risk categorisation g. Audit Title o. Audit observation description - the audit observation description will be further sub categorised into ▸ Condition ▸ Criteria ▸ Causes ▸ Consequences/Effect/Impact h. Recommendation	CIA/IA of IAU
2	After recording all the details, the same will be submitted to CIA of IAU for approval.	IA of IAU
3	CIA of IAU can either approve the draft audit report or return the same with remark. After approval of CIA the same will be published in AMS. Note:- The final draft audit report shall be submitted to audit unit within two weeks from the last of the field visit	System (Auto)
4	On return by IAU (CIA) the Internal Auditor can make required changes and re-submit the same to IAU (CIA).	CIA of IAU
5	Audit Unit will access the draft audit report from online AMS portal and submit management response against each para. Note:-Management shall submit the management response on draft audit report within two weeks from the date of receipt of the draft audit report.	Audit Unit
6	Audit report is finalised after analysing the Management Response received from audit unit. Note:- The final audit report shall be submitted to audit unit within two weeks from the date of receipt of management response.	IAU
7	Final Audit Report sent to head of Ministry/ Autonomous Body/ Dzongkhags with a copy to CCA.	IA/CIA of IAU
8	Endorsement of final audit report by head of Ministry/ Autonomous Body/ Dzongkhags.	Head of Ministry/ Autonomous Body/ Dzongkhags

Sl.	Step	Actor/ Competent Authority
9	Final Audit Report made available to Audit Unit after endorsement automatically.	System

2.2.2 Functional Requirement Specification

FRS Sr. No.	Sub-Module	Requirement Description
FRS_AUER_001	Access of online system	▶ System will allow the following role-based access to the authorized users: ● CIA of IAU:allocate specific work to team members, Verification/ Rejection of audit observations, Submission of audit report for endorsement to head of government agency. ● Internal Auditor: view the list of work allocated to them, record/ modify audit observations in the system and submit to CIA of IAU for verification. ● Audit Unit: view audit report/ paras, submit management response.
FRS_AUER_002	Master data management	▶ List of work to be allocated to team members can be configured in the system which includes list of documents, registers, books of accounts, list of procurement, etc.
FRS_AUER_003	Entry Meeting and Allocation of work	▶ CIA/ IA of IAU can record and submit entry meeting details. ▶ CIA of IAU can approve the entry meeting. ▶ Once the Opening Meeting is recorded then system will allow recording of information related to auditors joining/ leaving audit party. ▶ System will allow printing of joining/ leaving letter. ▶ The CIA of IAU select a team member from available list and allocate specific work of current unit to the team member through the system. ▶ The team members can view the list of work allocated to him/ her by logging in to the system.
FRS_AUER_004	Audit Execution	▶ The system will provide facility to record observation of auditors through audit execution checklist. ▶ System will allow configuration of type of audit wise checklist. ▶ User will select a process from available list. System will fetch a list of available heads under the selected process. ▶ The system will then populate the list of questions relevant to the type of audit unit. ▶ User need to select response (Yes/ No/ N/A) against each question and save. ▶ User can create audit memo/audit observations against each question answered as no. ▶ User need to capture following information while creating a memo: ● Audit Unit ● Type of Audit ● Audit Year

FRS Sr. No.	Sub-Module	Requirement Description
		• Audit Period • Memo/audit observations Date (Auto from session) • Memo/audit observations Number (Auto) • Memo/audit observations Type • Amount Involved • Observation Type • Audit Process, Head • Memo/audit observations title • Description – further sub categorised into i. Condition ii. Criteria iii. Causes iv. Consequences/Effect/Impact • Attachment if any ► User can also create audit memos/observations directly in the system for a selected audit unit for a specific review period. ► User submits the created memo/observations for approval to CIA of IAU. At this point the status will be changed to SENT_FOR_APPROVAL. ► When the memo/observations are approved by the CIA of IAU the status will be changed to APPROVED. ► Once the Audit Memo/observations is approved by the CIA of IAU it will be sent automatically to audit unit for response. The status of the memo/observations will be changed to SENT_TO_UNIT. ► After receiving the memo from CIA of IAU the audit unit submits response against it. The status will be changed to RESPONSE_RECEIVED. ► After receiving response from audit unit, the Internal Auditor decides whether the memo/observations need to be dropped or to be converted to para. If the para is dropped by the Internal Auditor, then the status of the memo/observations will be changed to DROPPED. If the memo/observations are converted to para then the status will be changed to CONVERTED_TO_PARA. Any memo/observations can be converted to para at any point of time. If response is not received on time, then also a memo/observation is automatically converted to para updating its status to CONVERTED_TO_PARA. ► User will be able to see list of audit memos/observations created by him and his team member. ► Any memo/observations can be converted to para at any point of time by the user. If response is not received on time, then also a memo/observation is automatically converted to para updating its status to CONVERTED_TO_PARA. Following information will be recorded while creating a para: • Audit Unit

FRS Sr. No.	Sub-Module	Requirement Description
		• Type of Audit • Audit Year • Review Period • Audit Party • Auditor • Observation Type • Audit Process, Head • Observation Type • Amount Involved • Amount Recoverable • Para Category (Auto) • Para Risk Priority • Para Title • Detail Description of Para - the audit observation description will be further sub categorised into ▶ Condition ▶ Criteria ▶ Causes ▶ Consequences/Effect/Impact ▶ Recommendation • Attachments • Related Section • Concerned Official (Name, Designation, email id) • Timeline ▶ System will also provide facility to define observation type wise input parameters against which the Internal Auditor will capture data. Such configurations will be done by the administrator only. While defining a parameter user will mention details like Label, Input Type (Text/ List/ Checkbox/ Option), Data Source/ Fixed Data List, Is Compulsory, Help Text, Validation etc.
FRS_AUER_005	Audit Execution	▶ Internal Auditor conduct audit and record audit para in the system directly and submit to CIA of IAU for verification. ▶ The system will also allow performing performance audit and testing of internal controls of audit units. ▶ In case of performance audit and testing of internal control the system will allow the Internal Auditor to evaluate audit organisations through pre-defined check lists. These check lists (parameters, allowed value/ value-sets) can be configured in the system. Discrepancies recorded against parameters will generate audit paras. ▶ The customized checklist depends upon the type of audit that can be

FRS Sr. No.	Sub-Module	Requirement Description
		configured in the system. For example, the performance audit is to be performed for topic/theme/program/scheme and hence for every such type of topic/theme/program/scheme a specific checklist will be required to execute the audit. Hence, internal auditor will prepare these specific checklists based on his professional judgement and upload it into the system. ► User will enter/select appropriate values/options against each parameter. ► User can provide descriptive remark against each parameter. ► User can also upload required documents against each parameter.
FRS_AUER_006	Configuration	► The default verifier/approver of an audit para is the CIA of IAU. The system will also allow configuration of default verifier and approver.
FRS_AUER_007	Audit Execution	► The system will provide facility of marking an observation as Verified/ Rejected (with reason) by CIA of IAU.
FRS_AUER_007	Audit Execution	► On rejection of an audit observation the system will forward the audit observation to the concerned Internal Auditor for making required modification as per remark of the CIA of IAU.
FRS_AUER_008	Audit Execution	► The IA of IAU will do necessary modification in the audit observation as per remark of the verifier/ approver and re-submit the same for verification.
FRS_AUER_009	Reporting	• IA of IAU will select an audit unit and review period for recording following details to complete preparation of draft audit report: • Auditee Details • List of Officials met • Audit party details • Audit details (Scope and Coverage) • Audit Para type • Audit para risk categorisation • Audit Title • Audit observation description - the audit observation description will be further sub categorised into ○ Condition ○ Criteria ○ Causes ○ Consequences/Effect/Impact • Recommendation ► After recording all the details, the same will be submitted to CIA of IAU for approval. ► IAU (IA/ CIA) can either approve the draft audit report or return the same with remark. After approval of CIA of IAU the same will be published in AMS. (Note: - The final draft audit report shall be

FRS Sr. No.	Sub-Module	Requirement Description
		submitted to audit unit within two weeks from the last of the field visit) ▶ Audit Unit will access the draft audit report from online AMS portal and submit Management Response against each observation.
FRS_AUER_010	Reporting	▶ The system will provide facility of marking an audit report as Approved/ Rejected (with reason) by CIA of IAU.
FRS_AUER_011	Reporting	▶ On approval by the approver the system will publish the audit report in AMS portal. ▶ The audit report willhave separate sections for reporting observations.
FRS_AUER_012	Reporting	▶ The audit unit can access the approved audit report from online AMS portal and submit para/ observation wise management response. (Note: Management shall submit the management response on draft audit report within two weeks from the date of receipt of the draft audit report.) ▶ Audit report is finalized after analyzing the Management Response received from audit unit. (Note: - The final audit report shall be submitted to audit unit within two weeks from the date of receipt of management response.) ▶ Final Audit Report sent to head of Ministry/ Autonomous Body/ Dzongkhags with a copy to CCA. ▶ System provides facility for endorsement of final audit report by head of Ministry/ Autonomous Body/ Dzongkhags. ▶ Final Audit Report made available to Audit Unit after endorsement automatically.
FRS_AUER_013	Daily Diary Maintenance	▶ The system will allow Internal Auditor take entry in online daily diary at every day-end on the basis of activities performed against assigned work. ▶ The system will allow CIA of IAU to acknowledge the online daily diary entries recorded by Internal Auditor.
FRS_AUER_014	Closing Meeting	▶ IA/CIA of IAU will record the details of exit/ closing meeting. Following information are recorded in the system: • Name of the Audit Unit • Audit Year • Meeting Date • Members Present (Name, Designation, email id) • Points Discussed • Attachment if any ▶ Information recorded is submitted to CIA of IAU for approval. ▶ CIA of IAU views the submitted information and take necessary action (Approve/ Reject with Remark). ▶ Once the Closing Meeting is recorded then system will not allow recording of daily diary details.
FRS_AUER_015	General	▶ On saving the audit report by draft audit report the record will be assigned with a unique audit report id as follows: <AUDIT_UNIT_CODE>+<YEAR>+<SL> ▶ On saving any audit observation by each IAU an unique ID will be

FRS Sr. No.	Sub-Module	Requirement Description
		assigned to every observation in following format: <AUDIT_REPORT_ID>+<OBSERVATION_SL>
FRS_AUER_016	Retrieve information	▶ System will allow retrieving audit report information after entering year, IAU, unit type, unit name etc.
FRS_AUER_017	System functionalities	▶ System will retain the saved information in case of any error or abrupt closing of current page
FRS_AUER_018	Reports	▶ The system will allow the users to print and download the annual audit report
FRS_AUER_019	Reports	▶ System will allow to generate the reports based on certain pre-defined parameters
FRS_AUER_020	System functionalities	▶ System will have data entry module for master data entry with roles for information creator and verifier
FRS_AUER_021	System notifications	▶ The system will display appropriate messages like: ▶ Confirmation message: Unique Audit Report id generated; Audit Report details updated; Email/ SMS notification sent etc. ▶ Error message in case of unsuccessful transmission: Audit Report id cannot be edited; etc. ▶ Messages pertaining to role based access controls will also be displayed like: You are not authorized to perform this action etc.

2.3 Follow-Up & Compliance Management

2.3.1 Process Definition

Process Definition: Follow-up & Compliance

Sl.	STEP	ACTOR/ COMPETENT AUTHORITY
1	Audit Unit submits action plan on compliance of audit observations. Observation wise time lines for compliance is submitted. Note: Audit unit will have to submit the action plan within 30 days from the date of receipt of final audit report.	Audit Unit
2	Generate the list of units where compliance is due/ over-due. Send system generated SMS/ e-Mail notification to audit units for submission of compliance. Reminders can be sent to audit units 2 week before expiry of para wise allotted timeline by system. Notification will also be sent to secretary/head of agency after expiry of para wise given timeline by the audit unit.	IA/ CIA of IAU
3	Audit units acknowledge the receipt of follow-up communication in the system.	Audit Unit
4	Audit unit submits para/ observation wise compliance to IAU through AMS or through letter. Audit unit will also provide the supporting document against the observations which is implemented or complied for internal auditor to verify and update the compliance status accordingly.	Audit Unit
5	IA/ CIA of IAU records the compliance details received against specific para and submits for approval. Following details will be recorded: a. Letter No b. Letter Date c. If Recovery Required (Auto) d. Amount Recoverable (Auto) e. Amount Recovered f. % Recovered (Auto) g. If Complied h. Compliance Date i. Remark (If Any) j. Attachments	IA/ CIA of IAU
6	IA/ CIA of IAU in-charge reviews the compliance details received against paras and take required action. a. Reject the compliance (Para not dropped) b. Approve the compliance (Para dropped)	IA/ CIA of IAU

Sl.	STEP	ACTOR/ COMPETENT AUTHORITY
7	System will allow generation of Annual Audit Report where observations of all units under an IAUs will be compiled.	IA/ CIA of IAU
8	Submission of Annual Audit Report to CCA.	IA/ CIA of IAU
9	System will send the status of audit observation and recommendation implementation status of audit unit to secretary / head of respective government agency periodically.	System

2.3.2 Functional Requirement Specification

FRS Sr. No.	Sub-Module	Requirement Description
FRS_FUCM_001	Access of online system	▶ System will allow the following role-based access to the authorized users: • IA/ CIA of IAU: Generate compliance due list, send reminder notification to audit units for submission of compliance, records the compliance details received against specific para. • Audit Unit: submit action plan, acknowledge the receipt of follow-up communication, submits para wise compliance etc. • IA/ CIA of IAU: review the compliance details received against specific para and take required action
FRS_FUCM_002	Follow-Up	▶ Audit Unit submits action plan on compliance of audit observations. Observation wise time lines for compliance is submitted. (Note: Audit unit will have to submit the action plan within 30 days from the date of receipt of final audit report.) ▶ IA/ CIA of IAU generates the list of units where compliance is due/ over-due. ▶ System should allow configuring the allowed timelines by administrator.
FRS_FUCM_003	Follow-Up	▶ IA/ CIA of IAU sends system generated SMS/ e-Mail notification to audit units for submission of compliance. ▶ Reminders can be send to audit units 2 weeks before expiry of para wise allotted timeline by system. ▶ Notification will also be sent to audit units after expiry of para wise allotted timeline by system.
FRS_FUCM_004	Follow-Up	▶ Audit units acknowledge the receipt of follow-up communication in the system.
FRS_FUCM_005	Compliance	▶ Audit unit submits para wise compliance to IAU through AMS or through letter.
FRS_FUCM_006	Compliance	▶ IA/ CIA of IAU records the compliance details received against specific para and submits for approval. Following details will be recorded: a. Letter No

FRS Sr. No.	Sub-Module	Requirement Description
		b. Letter Date c. If Recovery Required (Auto) d. Amount Recoverable (Auto) e. Amount Recovered f. % Recovered (Auto) g. If Complied h. Compliance Date i. Remark (If Any) j. Attachments
FRS_FUCM_007	Compliance	▶ IA/ CIA of IAU reviews the compliance details received against specific para and take required action: ▶ Reject the compliance (Para not dropped) ▶ Approve the compliance (Para dropped)
FRS_FUCM_008	Compliance	▶ CCA can view compliance status of all IAUs in a single report.
FRS_FUCM_009	Compliance	▶ IA/ CIA of IAU communicates the para wise action taken report/ compliance report to audit unit. ▶ System will allow generation of IAU/ Unit wise Performance Report. ▶ System will send the status of audit observation and its implementation status of audit unit to secretary / head of respective government agency periodically.
FRS_FUCM_010	General	▶ On saving the audit compliance the record will be assigned with a unique audit compliance id as follows: <OBSERVATION_ID>+<COMPLIANCE_SL>
FRS_FUCM_011	Retrieve information	▶ System will allow retrieving audit compliance information after entering year, unit type, unit name etc.
FRS_FUCM_012	System functionalities	▶ System will retain the saved information in case of any error or abrupt closing of current page
FRS_FUCM_013	Reports	▶ The system will allow the users to print and download the annual audit compliance report
FRS_FUCM_014	Reports	▶ System will allow to generate the reports based on certain pre-defined parameters
FRS_FUCM_015	System functionalities	▶ System will have data entry module for master data entry with roles for information creator and verifier
FRS_FUCM_016	System notifications	▶ The system will display appropriate messages like: ▶ Confirmation message: Unique audit compliance id generated; audit compliance details updated; Email/ SMS notification sent etc. ▶ Error message in case of unsuccessful transmission: Audit Report id cannot be edited; etc. ▶ Messages pertaining to role based access controls will also be displayed like: You are not authorized to perform this action etc.

2.4 MIS Report

Every Government organization aims to have an effecting reporting/MIS tool that provide information that organizations require to manage themselves efficiently and effectively. This tool aims to provide decision support to the CCA with various types of MIS reports. The system will consolidate the audit observations recorded by different IAUs and allow submission of consolidated report to CCA. The system will also provide facility to consolidate all audit observations at CCA level. CCA can generate various type of MIS and decision support reports like Category wise pendency report, category and location wise financial impact, plan vs actual audit execution etc. Collection of such information will gradually build a knowledge base on audit management which will help the CCA/RGoB in decision making and policy making. Besides pre-defined reports the system also provides facility to generate user-definable reports where user can define their own reports by dynamically selecting required fields and selection criteria. Important sub-modules of Follow-up and Compliance Module are as follows:

- Consolidation of Audit Observation by IAUs
- Submission of Consolidated Report to CCA
- Generation of IAU/ Unit wise Performance & MIS Reports

2.5 Dashboard

The system will provide separate dashboards for different type of users like CCA, IAUs, Ministry of Finance, Audit Party and Audit Units etc. The dashboard will enable the users to view performance of their concerned units at a glance. User Dashboards will be available to concerned users after secure login to the system. Information in the dashboard will be presented graphically through charts, tables, metrics, maps and widgets. The dashboard will show various analytical information like year & unit type wise pending paras, year & unit type wise closed paras, year wise unit type wise para type wise analysis of open and closed paras etc. The dashboard will also provide information on health and performance of different units. Important sub-modules of this module are as follows:

- CCA Dashboard
- Finance Ministry Dashboard
- IAUs Dashboard
- Auditee Units Dashboard
- Common User Profile

2.6 Integration

Integration with External Applications:The system will be integrated with external systems like MYRB and PEMS etc. System integration can be done either through web-services or through file sharing method. Unique code of the audit units which is maintained in external application will be used to retrieve information from these applications.

Non-functional Requirements

3.1 Performance Requirements

The performance level is defined as the responsiveness of the proposed application and shall be quantified on the basis of load and response time of the system. It would be a key challenge for the developers and operations and maintenance team to maintain the performance level as the use of the system would increase leading to increase in number of users and data volumes. The performance of the system to the end user would also depend on the quality of connectivity and uptime of the underlying infrastructure. The proposed architecture should take care of the application performance requirements by implementing required techniques like load balancing, caching etc. The table below describes the performance requirements of the system:

Action	Response Time
Loading of static pages	90% of static pages should load within 5 seconds
User operation of data	5 – 10 seconds
Transactions (query/ update)	10 – 30 seconds
Search	30 seconds

2.2 Security Requirements

The application will store identities of Government Officers and other stakeholders, and workflows are some areas which are critical with respect to security. Adequate safety measures to be incorporated during development stage to prevent vulnerabilities and build a secure code for these services. The following security considerations are to be made:

- **User Level Security:** Restricted areas of the application shall be accessible through pre-defined user access rights.
- **Database Level Security:** Database security should provide different layers of database users with overall control of database security administrator, only authorised database administration users with assigned privilege shall be allowed to access database. A separate audit trail should be maintained for any direct modification, deletion and addition in RDBMS database in database structure or records. User, even the database administrator should not be allowed to tamper with audit log.
- **Network Level Security:** Network traffic shall be encrypted using SSL.
- **Infrastructure Level Security:** Application infrastructure shall be hosted in a DMZ & firewall and IPS shall be installed to detect malicious activities.
- Prevent SQL Injection Vulnerabilities for attack on database.

2.3 Audit Trail & Access Control

It is required to build a complete audit trail of all transactions (add, edit and delete) using transaction log reports, so that errors in data – intentional or otherwise can be traced and reversed. Access Controls must be provided to ensure that the databases are not tampered or modified by the system operators. Implement data security to allow for changes in technology and business needs. Internal Users (Department Users / Operators) should not be able to login to the application, without providing login credentials. Database server access shall be provided through appropriate access control mechanism. User groups would be created at database server for allowing access to various data repository. Users should be granted access to information, data, devices, processes/daemons, audit files and software on a "need to know" basis. Access will be restricted according to the user's requirement to read, write or execute data or software on the basis of least privilege to achieve the desired function. The proposed solution must allow controlling actions and access to resources of all users including privileged accounts such as root / administrator. There should not be any mechanism to delete data or information. All activities of deletion should lead to data being moved from the main place to a secondary

place earmarked for storing deleted data. Under no circumstances data should be expunged. The system should support Role-based Administration and Role Based & Rule Based User Provisioning.

2.4 Maintainability

Maintainability is defined as the ease with which the software system and components can be modified to correct faults, improve performance or other attributes. It is envisaged that the application shall have high degree of maintainability. Maintenance activities required for smooth and efficient functioning of system are given as below:

- **Corrective Maintenance:** Performed to correct discovered bugs/ issues
- **Adaptive Maintenance:** Performed to keep the system usable in case of changing environment
- **Preventive Maintenance:** Performed to correct latent faults in a software product
- **Perfective Maintenance:** Performed to improve performance or maintainability of the system

2.5 Integration with external systems

The system should have the openness to be integrated with any external system as and when required. The technology stack used for development of the application must support service-oriented architecture for publishing and consumption web-services. The application should be able to consume web-services of any other external application in-order to retrieve or submit information as per requirement. The application should also support publishing web-services for use of external systems if required.

2.6 Software Development methodology & platform

The proposed system should leverage best IT practices, guidelines and standards. The system should be designed and developed on bespoke model. Software Development Life Cycle should be followed while developing the application. Open standard technology architecture with open source products should be used for development of the proposed application.

2.7 Cyber Security Audit

All the modules/sub-modules of the proposed system should be security audited by any cert-in certified cyber security auditor. Proper security certificate should be obtained from the auditor agency before deployment of the application. This will ensure that critical information of government is properly protected from unauthorized access and/or update.

2.8 Miscellaneous

The web pages of this application should support at least browsers like Internet Explorer, Mozila Firefox, Opera and Chrome. The system should provide data export facility to popular formats such as MS Office and Open Office, PDF, XML etc. Business Rules in the system should be platform independent. Functional authorities, not IT resource persons, should be able to manage all the business rules and system configurations.

21 Appendix II:

Functional requirement Specifications prepared by CCA.

Note:*Following provisions have been prepared for both: COTS or BESPOKE applications. Provisions not applicable in either approach may be ignored:*

1. IAMS Homepage (Dash Board)

1.1. The IAMS Homepage will be the landing page. The consultant will work with the CCA/MoF to secure the necessary domain name. The Homepage will carry the System Name/Branding, to provide login access for Internal Auditors, Internal Audit supervisors, CCA officials, Head of agencies and PM Office's focal person to provide internal audit work-related information. The consultant shall propose an effective layout to present the function/information described above.

1.2. The homepage display Information/Functions shall include the following:

1.2.1. Login Validation for Internal Auditors, Internal Audit supervisors, CCA officials, Secretaries and PM Office.

1.2.2. Important Announcements, Circulars and Notification of Government offices.

1.2.3. Important Announcements and Notification from CCA.

1.2.4. Registration of IAMS user

1.2.5. The Homepages shall also provide online user manuals and FAQs. The consultant will develop the user manuals and work with CCA on the FAQs.

1.3.Registration

1.3.1. The IAMS Homepage will provide registration and it should be accessible to all IAMS users. However, all the users are required to register on IAMS before being able to use the system. IAMS users will be: Internal Auditors, Internal Audit supervisors, CCA officials, Head of agencies and PM Office focal person.

1.3.2. During the registering, IAMS will capture information such as:

- ✓ Name of concerned officer
- ✓ Employee ID of the officer
- ✓ Designation of the concerned officer
- ✓ Official Email ID
- ✓ Mobile Number
- ✓ Contact Address (official)

1.3.3. Before the registration, eligibility verification for different user's registration will be done offline by an IAMS Administrator.

1.3.4. When the Registration is successful, a notice will be given with the User ID and Password.

1.3.5. If accepted, an email notification will be sent to the USER with the user ID and password.

1.3.6. If rejected, the IAMS Admin will select the reasons from a predefined list and send an email notification to the applicant.

1.3.7. When user login for first time IAMS will be prompted through and OTP to change the password before being able to use the system.

1.3.8. IAMS shall have options to change and retrieval of the password.

1.3.9. Password Retrieval Function

1.3.9.1. IAMS shall have automated password retrieval functions for all the user once they have successfully registered.

1.4.IAMS Admin

1.4.1. IAMS shall have administrators from CCA, MoF. These administrators will verify and approve the accounts for all the user.

1.4.2. IAMS shall also have functions to update and delete users.

1.4.3. This Administrator shall also be able to assign system-level access by Agency, Roles, Functions and Fields such as IA supervisor or Internal Auditor.

2. User's Homepage (dashboard)

2.1. The user Logs in via the IAMS Homepage, the user should be directed to their respective Homepage.

2.2. When an IA logs in via the IAMS Homepage, the IA should be directed to IA Homepage.

2.3. When an IA supervisor logs in via the IAMS Homepage, the IA supervisor should be directed to Supervisor Homepage.

2.4. When the head of agency logs in via the IAMS Homepage, the head of agency should be directed to Individual agency report Homepage.

2.5. When CCA officials logs in via the IAMS Homepage, the CCA officials should be directed to CCA Homepage.

2.6. When PMO officials logs in via the IAMS Homepage, the PMO officials should be directed to PMO official Homepage.

2.7. All the user's Homepage will store relevant information/instructions as well as provide access to the respective user's information (such as Internal Audit plan, observations, recommendations, monitoring, follow-ups, history, outstanding tasks, completed tasks etc.)

2.8. All the user's Homepage will be the starting page for all functionalities as stated in individual Homepage.

3. Supervisor Homepage (dashboard)

3.1. Internal Audit Annual Plan

3.1.1. IAMS shall have provision for the supervisor to visit the previous year's Internal Audit Annual Plan and retrieve the Previous Year's Plan to develop/prepare the Current Year Plan through inclusion or exclusion of assignments.

3.1.2. Under the planning page, the supervisor shall strategize and develop an Annual Planning by establishing Internal Audit Strategy, identifying Audit Universe & Auditable Area.

3.1.3. The Audit universe includes financial and non-financial areas, that are subject to the control or the authority of the head of the agency.

3.1.4. The entities and elements comprising the audit universe should be grouped into units of auditable areas.

3.1.5. Auditable areas should be determined and identified by:

Organizational structure;	such as departments, divisions, and offices. A department may consist of several divisions with different programmes and activities which may be too large to be considered as one single auditable area because of the diverse functions performed by the various Divisions. Hence it may be preferable to identify each division as a primary auditable area.
Programme structure;	the specific programmes, sub-programmes, activities or functions undertaken by the agency. Often the organizational structure may reflect the programme structure.
Systems and processes;	systems and processes that may be common in all organizational units or those that cut across all organizational units. This normally includes support functions such as the accounting, payroll processes, procurement, human resources, information technology and other

	such functions.

3.1.6. The profile of an auditable area should be as per **Annex lll-1** (Internal Audit Manual, page no.65).

3.1.7. The auditable areas should be based on risk ranking developed on a series of prioritization criteria specified as per risk matrix, **Table III-2** (Internal Audit Manual, page no.60).

3.1.8. The prioritization criteria should carry weight to rank the auditable areas. The CCA will decide the weightage on the prioritization criteria. However, the following is an example,

- ✓ Complexity of operations (10%)
- ✓ Impact on RGoB or Bhutan (15%)
- ✓ Control environment (20%)
- ✓ Management interest (10%)
- ✓ Change in Policy/Process/Personnel (20%)
- ✓ Size of the operating unit (25%)

3.1.9. To provide the weight to the prioritization criteria, there should be a further mechanism in scoring point for the criteria based on 1 to 5 or High, Medium, and Low as per Internal Audit Manual (Page 61 and 62). For example, complexity of operations is assessed based on the following scores:

Score	Definition
1	operation is simple or routine
2	operation relatively simple, some training required
3	operation moderately complex, training, and detailed instruction required
4	operation is complex, the task can only be done by experienced employee
5	operation is very complex, a specialist in the field required

3.1.10. The prioritized auditable areas should be linked with the Resources and allocated accordingly by the supervisor. The resources consist of Financial and Human Resources.

3.1.11. Total available human resources for the year should be estimated based on the **Table lll-1** (Resources Allocation Plan for Financial year 20xx); Page No.56 of the Internal Audit Manual.

3.1.12. There should be provision for the supervisor to allocate the available human resources to the high-risk auditable areas for the engagement.

3.1.13. Along with the allocation of available human resources, the provision should be developed to allocate the budget required for the engagement and the budget should not exceed the approved budget for the year.

3.1.14. There should be additional provision if the approved budget is not adequate for the engagement. Depending on the severity of the engagement the additional budget can be requested to Department of National Budget through respective ministry or CCA.

3.1.15. The page should have provision to write the introduction, Audit Scope, Audit objectives, limitation/shortcoming, and name of Supervisor.

3.1.16. While developing the Internal Audit Annual Plan, the system should automatically provide 20% of human resources and budget for the Consulting and ad-hoc works and should be recorded in the Internal Audit Annual Plan.

3.1.17. The IAMS should automatically generate the Internal Audit Annual Plan in PDF and MS word formats depicting the following Topic:

1. Introduction
2. Audit Scope
3. Audit objectives
4. Name of Audit Staff
5. Detail Audit Engagement as per the **Table lll-3**: (Detailed Annual Audit Plan for the year 201X) as in page no.64 of the Internal Audit Manual.
6. Limitation/shortcoming
7. Signature of Head of the IA and Organization.

3.1.18. The page should have the option for delegation to subordinates to plan the Annual Internal Audit Plan.

3.1.19. After completion of Internal Audit Annual Plan, the supervisor should submit to the head of the organization for approval.

3.1.20. There should be provision for submission of subsequently edited IA Annual Plan (inclusion or exclusion) in annual plan to head of the organization for approval.

3.2. Audit Engagement

3.2.1. The head of IA unit should be able to select or prioritize the auditable area for the engagement from the IA annual plan.

3.2.2. The auditable area for the engagement should have a serial number or identification code for easy identification and to record the information.

3.2.3. There should be an option for the head to take up the engagement process by himself/herself or delegate the process to Internal Auditor/auditors under him/her.

3.3. **Audit Process**

3.3.1. The audit process should begin with the Audit Commencement and Control Record as per the **Index C**.

3.3.2. The record should contain the name of supervisor preparing the control record with the date as well as the provision for the approval.

3.3.3. Notify Auditee (an engagement letter). The IA supervisor should able to generate the engagement letter as given in the **Format I** attached.

3.3.4. The system should be able to send the email (an engagement letter) to the addressed auditee and the respective officials.

3.3.5. Once the IAU head has assigned IA team members for the specific engagement, the concerned internal auditor engaged in the assignment should be able to declare the Conflict of Interest though IA supervisor page or IA Homepage as in **Index CC-1**.

3.3.6. The system should be able to retrieve/generate the name of auditor who prepared the CoI with the date as well as the provision for the approval.

3.3.7. To have the overall knowledge of the auditee organization, the system should have the provision of Preliminary Survey as in **Index DD-I**. In subsequent years, the system should be able to provide the previous Preliminary Survey details which could be edited by the auditor but the original details will be preserved.

3.3.8. From the preliminary survey, the records should have a sufficient summary of the knowledge of organization and function/business as in **Index DD-II**.

3.3.9. The system should be able to retrieve/generate the name of auditor who prepared the Preliminary Survey and summary of knowledge of business as well as the provision for the approval.

3.3.10. The system should have an option for the Audit Project Risk Assessment and Fraud Risk Assessment.

3.3.11. Audit Project Risk Assessment should be able to assess project/activity's risk as per the audit engagement. The assessment should be based on **Index EE-1**. And there should be an option to add or delete the activities as per the engagement.

3.3.12. Like the risk assessment, the system should assess the fraud risk as per the Fraud Risk Assessment (**Index EE-2**);

3.3.13. The system should be able to retrieve/generate the name of auditor who prepared the Audit Project Risk Assessment and Fraud Risk Assessment as well as the provision for the approval.

3.4. Engagement Plan

3.4.1. There is difference between the Engagement Plan and IA annual plan. IA annual plan is for a year and Engagement Plan is for the specific audit engagement.

3.4.2. The Engagement Plan should be able to give a brief knowledge of the engagement and process to be followed during the engagement. The Engagement Plan should be as per Index FF-1.

3.4.3. The system should be able to retrieve/generate the name of auditor who prepared the Engagement Plan as well as the provision for the approval.

3.5. Entry Conference (Entry Meeting)

3.5.1. Recording of minutes of the opening conference (entry meeting) should be as per the Index FF-2.

3.5.2. The system should be able to retrieve/generate the name of IA supervisor preparing the Minutes of meeting for opening conference with date when it is prepared.

3.5.3. Once the minute is finalized, the IA supervisor should be able to send the finalized minutes to the members present during the opening conference (entry meeting) through system in PDF format via email. Therefore, system should have the provision for inserting recipient email IDs once the minute is generated.

3.5.4. The IA supervisor may delegate the task of recording minutes of meeting to an Internal Auditor. In such a case, the system should have the option to delegate this task by the IA Supervisor to the Internal Auditor.

3.6. Internal Audit Program and control.

3.6.1. According to the allocation of assignment/project/activities, the system should be able to generate Audit Program Control Sheet (APCS) as per Index GG.

3.6.2. The system should be able to retrieve/generate the name of auditor who prepared the APCS as well as the provision for the approval.

3.6.3. Along with the control sheet, the auditor should be able to develop Audit Program as per Index GG-1.

3.6.4. The system should be able to retrieve/generate the name of auditor who prepared the Audit Program as well as the provision for the approval.

3.7. **Internal Audit Checklists:**

3.7.1. The system should have checklists to confirm whether the required process is completed.

3.7.2. The planning checklist should be linked to the related working paper as given in **Index HH-1.**

3.7.3. The planning checklist should automatically update the checklist as and when the Internal Auditor updates the planning forms (**Index C to GG-1**) described above. The planning checklist should encompass the following broadheads;

- ✓ Audit Commencement;
- ✓ Preliminary Survey;
- ✓ Developing Engagement Plan;
- ✓ Developing Audit Programs;
- ✓ Document Management

3.7.4. The system should be able to retrieve/generate the name of auditor who prepared the Audit Planning Checklist as well as the provision for review by supervisor.

3.7.5. The system should automatically generate Internal Audit requisition form in the format of letter for Engagement with the option of entering details of required information.

3.8. **Internal Audit Observation Sheet**

3.8.1. The system should have an option to generate an Internal Audit Observation Sheet to record the finding/observation. The observation sheet should be in the format of **Index- BB**.

3.8.2. The system should be able to generate a different sheet for different finding/observation with specific code.

3.8.3. The system should be able to retrieve/generate the name of auditor who prepared the Internal Audit Observation Sheet as well as the provision for the approval.

3.8.4. The system should provide an option to fill the Fieldwork checklist by the audit/team leader and head of IAU to make sure the fieldwork is completed as in **Index HH-2**.

3.8.5. The system should have provision for IA Supervisor to send observation sheet to auditee for their comments via email.

3.9. Closing conference

3.9.1. Recording of minutes of the Closing conference (exit meeting) should be as per the **Index-I**

3.9.2. The system should be able to retrieve/generate the name of supervisor preparing the Minutes of meeting for closing conference with date.

3.9.3. Once the minute is finalized, the IA supervisor should be able to send the finalized minutes to the members present during the closing conference through system in PDF format via email. Therefore, system should have the provision for inserting recipient email IDs once the minute is generated.

3.9.4. The IA supervisor may delegate the task of recording minutes of meeting to an Internal Auditor. In such a case, the system should have the option to delegate this task by the IA Supervisor to the Internal Auditor.

3.10. Draft Internal Audit Report

3.10.1. With the internal audit working papers and observation sheet the system should be able to develop the draft internal audit report. The draft report should be in format of **Index-AA;**

3.10.2. The report should contain word "Confidential" on the top of the first page of the draft report.

3.10.3. The draft report should contain the person's details who prepared the draft report with the date as well as the provision for the review and approval with the date.

3.10.4. The draft report should contain the person's details who prepared the draft report with the date as well as the provision for the review and approval with the date.

3.10.5. The system should generate the draft report and send an email to the auditee after finalization

3.10.6. The email sent by IA supervisor to take the auditee should contain la link to a page within the draft report where they can provide their response (Management Response and Management Action Plan). The response and action plan provided by auditee should be in the format of **Annexure V-1** given on page no.94 of Internal Audit Manual. The auditee while preparing the Management Response and Action

Plan in **Annexure V-1** should be given the option to save draft, edit the saved response and finally submit the response to the auditor. But the auditee will have no access to the same page once the response is submitted. There should be a pop-up message to confirm to the auditee that submitting the response will be final, hence he/she will not have further access once the response or action plan is submitted.

3.10.7. The system should have an option to delegate the work of sending email to the auditee for management response, when an IA submits the draft report prepared by him which was delegated to him by the supervisor earlier after the report is approved by the supervisor.

3.10.8. The system should provide an option to fill the Reporting checklist by the audit/team leader and head of IAU to make sure that the reporting is completed as per **Index HH-3**.

3.11. Final Internal Audit Report

3.11.1. Once the management responses and action plans are received, the system should generate the final internal audit report as per **Index KK-1**.

3.11.2. The system should have a provision to insert the email addresses of the head of agencies, auditee, and other concerned officials to whom the final report is submitted.

3.11.3. The system should have a provision to confirm sending the email by IA supervisor at this stage.

3.12. Reporting (MIS)

3.12.1. The system should be able to generate and/or upload all the working papers or forms or reports and back-up in the database. Once the reports are finalized, the working papers or forms or reports should not have an option to edit or delete. However, the system should have an option to retrieve any working papers or forms or reports or individual observation/finding with a management action plan.

3.12.2. All the working paper/form/reports should contain the following meta data:

- ✓ Name of Form,
- ✓ Name of Organization,
- ✓ Engagement Name/Audit Topic,
- ✓ File No. and Audit period.

- ✓ Moreover, the working paper/form/reports should contain the person's details who prepared it with the date as well as the provision for the review and approval with the date.

3.13. **Consulting Services.**

3.13.1. IAMS shall give the right to the Supervisor to visit the previous and current year's consulting service documents or report but without editable rights.

3.13.2. The system should automatically generate Consulting Form as per **Index-L** to record the request received from the client and for future references.

3.13.3. The system should be able to record the COI (declare the Conflict of Interest) and able to print if required in the format of **Index CC-1**.

3.13.4. Notify Auditee (an engagement letter).
The internal auditor supervisor should be able to generate the Consulting engagement letter. If Consulting service required to go in the field. The engagement letter should be similar to audit engagement but with different subject and contents.

3.13.5. Consulting Observation Sheet
The system should generate a consulting observation sheet like in **Index BB** to record the finding/observation.

3.13.6. Reporting

3.13.6.1. The system should be able to generate all the working papers or forms or reports related to consulting service and back-up in the database. Once the reports are finalized, the working papers or forms or reports should not have an option to edit or delete. However, the system should have an option to retrieve any working papers or forms or reports or individual observation/finding.

3.13.6.2. All the Consulting working paper/form/reports should contain;

- ✓ Name of Form;
- ✓ Name of Organization;
- ✓ Name of consulting work;
- ✓ File No. and,
- ✓ Period.
- ✓ Moreover, the working paper/form/ consulting reports should contain details of supervisor preparing such documents with date when it is prepared.

3.13.6.3. The system should notify the head of agencies once the IA supervisor submits the Consulting report via email or in the system.

3.13.6.4. With the internal audit consulting working papers and finding/observation sheet the system should be able to develop internal audit consulting report.

3.13.6.5. The report should be in the following format;

- ✓ Cover page
- ✓ Date
- ✓ Name of File
- ✓ Address to (Client)
- ✓ Introduction/Brief Summary
- ✓ Main report

1. Introduction
   - 1.1. Purpose of consulting
   - 1.2. Scope of Consulting
   - 1.3. Methodology or Approach
   - 1.4. Limitations
2. Background
3. Prior issues
4. Observations/Case
   - 4.1. Objective 1
   - 4.2. Objective 2
5. Overall recommendation
6. Conclusion

3.14. Monitoring and follow-up

3.14.1. The system should have a database for all the observation/finding along with management responses and action plan. There should be an option to indicate/mark in the database when the management has implemented the recommendations.

3.14.2. The Head of IAU should be able to search and check the observation, whether the management has implemented the recommendation as per their action plan as initial, action in progress and completed.

3.14.3. When the recommendations are not implemented then there should be an option to send reminder through email automatically after every 2 months.

3.14.4. The system should also record all the correspondences for future reference.

3.14.5. The system should generate monitoring and follow-up report monthly/bi-annually/annually/report wise.

4. IA Homepage

Note: *Reference of **Indexes and Annexures** from IA supervisor page are made wherever relevant under IA homepage as well. The only difference in indexes/Annexures (which are formats for different phases of audit Lifecyle) under this page is the requirement for IA to submit for approval to IA supervisor and Supervisor to approve the same. Hence indexes or annexures in IA home page will have signing off phrase such as **Prepared by** and **Approved by**.*

4.1. Internal Audit Annual Plan

4.1.1. IAMS shall give the right to the Internal Auditors to visit the previous year's Internal Audit Annual Plan, and Plan for the current year as in IA supervisor's page.

4.1.2. When the supervisor assigns Internal Auditors to work on the IA plans, the system should provide rights to the IA to formulate the IA Plan otherwise it should be restricted; However, system should not allow amendment of the current IA plan (inclusion and exclusion of assignments) to the IA. This should be restricted to the supervisor only.

4.1.3. Under the planning page, if the supervisor delegates the planning activity to the Internal Auditors, the IA shall strategize and develop an Annual Internal Audit Plan by establishing Internal Audit Strategy, identifying Audit Universe & Auditable Area.

4.1.4. The Audit universe includes financial and non-financial area, that are subject to the control or the authority of the head of the agency.

4.1.5. The entities and elements comprising the audit universe should be grouped into units of auditable areas.

4.1.6. Auditable areas should be determined and identified by:

Organizational structure;	such as departments, divisions, and offices. A department may consist of several divisions with different programmes and activities which may be too large to be considered as one single auditable area because of the diverse functions performed by the various Divisions. Hence it may be preferable to identify each division as a primary auditable area.
Programme structure;	the specific programmes, sub-programmes, activities or functions undertaken by the agency. Often the organizational structure may reflect the programme structure.
Systems and	systems and processes that may be common in all organizational

processes;	units or those that cut across all organizational units. This normally includes support functions such as the accounting, payroll processes, procurement, human resources, information technology and other such functions.

4.1.7. The profile of an auditable area should be as per **Annex lll-1B**, Page No.65 of Internal Audit Manual.

4.1.8. The auditable areas should risk ranking based on a series of prioritization criteria specified as per risk matrix, **Table III-2,** Page No.60 of Internal Audit Manual.

4.1.9. The prioritization criteria should carry weight to rank the auditable areas. The CCA will decide the weightage on the prioritization criteria. However, following is an example;

- ✓ Complexity of operations (10%)
- ✓ Impact on RGoB or Bhutan (15%)
- ✓ Control environment (20%)
- ✓ Management interest (10%)
- ✓ Change in Policy/Process/Personnel (20%)
- ✓ Size of the operating unit (25%)

4.1.10. To provide the weight to the prioritization criteria, there should be a further mechanism in scoring point for the criteria based on 1 to 5 or High, Medium, and Low as per Internal Audit Manual (Page 61 and 62). Example: Complexity of operations:

Score	Definition
1	operation is simple or routine
2	operation relatively simple, some training required
3	operation moderately complex, training, and detailed instruction required
4	operation is complex, the task can only be done by experienced employee
5	operation is very complex, a specialist in the field required

4.1.11. The prioritization auditable areas should be linked with the Resources and allocated accordingly by the IA. The resources consist of Financial and Human Resources.

4.1.12. Total available human resources for the year should be estimated based on the **Table lll-1B** (Resources Allocation Plan for Financial year 20xx), Page No.56 of the Internal Audit Manual.

4.1.13. There should be provision for allocation of the available human resources to the high-risk auditable areas for the engagement.

4.1.14. Along with the allocation of available human resources, the provision should be developed to allocate the budget required for the engagement and the budget should not exceed the approved budget for the year.

4.1.15. There should be additional provision if the approved budget is not adequate for the engagement. Depending on the severity of the engagement the additional budget can be requested to Department National Budget through respective ministry or CCA.

4.1.16. The page should have provision to write the introduction, Audit Scope, Audit objectives, limitation/shortcoming, and name of IA.

4.1.17. The IAMS should automatically generate the Internal Audit Annual Plan in the form of PDF and MS word consisting following Topic;

1. Introduction
2. Audit Scope
3. Audit objectives
4. Name of Audit Staff
5. Detail Audit Engagement as per the Table lll-3: Detailed Annual Audit Plan for the year 201X of the Internal Audit Manual.
6. Limitation/shortcoming
7. Signature of Head of the IA and Organization.

4.1.18. After completion Internal Audit Annual Plan, the IA should submit to the head of IAU for approval.

4.1.19. The system should be able to retrieve/generate the name of auditor who prepared the working papers for IA annual plan along with date and approval by supervisor.

4.2. Audit Engagement

4.2.1. The IA homepage should provide automatic engagement notice to the IA for the upcoming assignment.

4.2.2. When the supervisor assigns Internal Auditors to work on the Audit process, then the system should provide rights to the IA to formulate the Audit process described below;

4.3. Internal Audit Process

4.3.1. The audit process should begin with the Audit Commencement and Control Record as per the **Index C**.

4.3.2. The record should contain the name of IA preparing the control records with the date as well as the provision for the approval.

4.3.3. Once the IAU head has assigned IA team members for the specific engagement, the concern internal auditor engaged in the assignment should be able to declare the Conflict of Interest through IA supervisor page or IA Homepage as per **Index CC-1**.

4.3.4. The system should be able to retrieve/generate the name of auditor preparing the CoI date as well as the provision for the approval.

4.3.5. To have the overall knowledge of the auditee organization, the system should have the provision of Preliminary Survey as in **Index DD-I**. In subsequent years, the system should be able to provide the previous Preliminary Survey details which could be edited by the auditor but the original details will be preserved.

4.3.6. From the preliminary survey, the records should have a sufficient summary of the knowledge of organization and function/business as in **Index DD II**.

4.3.7. The system should be able to retrieve/generate the name of auditor preparing the Preliminary Survey and summary Knowledge of business with date as well as the provision for the approval.

4.3.8. The system should have an option for the Audit Project Risk Assessment and Fraud Risk Assessment.

4.3.9. Audit Project Risk Assessment should be able to assess project/activity's risk as per the audit engagement. The assessment should be based on **Index EE-1**. And there should be an option to add or delete the activities as per the engagement.

4.3.10. Like the risk assessment, the system should assess the fraud risk as per the Fraud Risk Assessment (**Index EE-2**);

4.3.11. The system should be able to retrieve/generate the name of auditor preparing the both Audit Project Risk Assessment and Fraud Risk Assessment with date as well as the provision for the approval

4.4. **Engagement Plan,**

4.4.1. There is difference between the engagement plan and IA annual plan. IA annual plan is for a year and engagement plan is for a specific audit engagement.

4.4.2. The engagement plan should be able to provide brief knowledge of the engagement and process to be followed during the engagement. The engagement plan should be as per Index **FF-1**.

4.4.3. The system should be able to retrieve/generate the name of auditor preparing the Engagement Plan with date as well as the provision for the approval.

4.5. **Entry Conference (Entry Meeting)**

4.5.1. When the Internal auditor is delegated by the IA supervisor to record the minutes of meeting entry meeting, IA should be able to records the minutes of meeting of the closing conference as per **Index FF-2** through the system.

4.5.2. The system should be able to retrieve/generate the name of Internal auditor preparing the Minutes of Opening Conference (entry meeting) with date as well as the provision for the approval by the supervisor.

4.5.3. Once the minute is approved by the supervisor, the IA should be able to generate the final minutes in PDF formats.

4.5.4. The system should provide an option to send the minutes generated in PDF format to all members present during the entry meeting via email. Therefore, the system should have provision to insert email IDs of members present during the meeting.

4.6. **Internal Audit Program and Control**

4.6.1. According to the allocation of assignment/project/activities, the system should be able to generate Audit Program Control Sheet (APCS) as per Index **GG.**

4.6.2. The system should be able to retrieve/generate the name of internal auditor preparing the APCS with the date as well as the provision for the approval.

4.6.3. Along with the control sheet, the auditor should be able to develop the Audit Program as per **Index GG-1.**

4.6.4. The system should be able to retrieve/generate the name of internal auditor preparing the Audit Program with the date as well as the provision for the approval.

4.7. **Internal Audit Checklists;**

4.7.1. The system should have checklists to confirm whether the required processes are completed.

4.7.2. The planning checklist should be linked to the related working paper as in **Index HH-1**.

4.7.3. The planning checklist should automatically update the checklist as and when the Internal Auditor updates the planning forms (**Indexes C to GG-1**). The planning checklist should encompass the following broadheads;

- ✓ Audit Commencement
- ✓ Preliminary Survey
- ✓ Developing Audit Plan
- ✓ Developing Audit Programs
- ✓ Document Management

4.7.4. The system should be able to retrieve/generate the name of internal auditor preparing the Check List with the date as well as the provision for the approval.

4.7.5. The IA homepage should give the topics/activates for the different Internal Auditor take-up under one assignment.

4.7.6. The system should automatically generate Internal Audit requisition form in the format of letter for Engagement with an option of entering datils of required information.

4.8. **Audit Observation Sheet**

4.8.1. The system should have an option to generate an Internal Audit Observation Sheet to record the finding/observation. The observation sheet should be in the format of **Index- BB**;

4.8.2. The system should be able to generate a different sheet for different finding/observation with specific code.

4.8.3. The system should be able to retrieve/generate the name of internal auditor preparing the observation sheet with date and provisional for approval by IA supervisor.

4.8.4. The system should provide an option to fill the Fieldwork checklist by the audit/team leader and head of IAU to make sure the fieldwork is completed as in **Index HH-2**.

4.8.5. The system should have provision for Internal Auditor to send observation sheet to the auditee for their comments via e-mail.

4.9. **Closing conference (Exit meeting)**

4.9.1. When the Internal auditor is delegated by the IA supervisor to record the minutes of meeting, IA should be able to records the minutes of meeting of the closing conference as per **Index-I** through the system.

4.9.2. The system should be able to retrieve/generate the name of Internal auditor preparing the Minutes of meeting for exit meeting with date and the name of supervisor approving the minutes along with date.

4.9.3. Once the minute is finalized, the IA should be able to submit the same to the IA supervisor for approval. After the minute is approved by the IA Supervisor, the internal auditor should able to generate the minutes in PDF format and email it to all members present during the exit meeting. Therefore, system should have the provision for inserting recipient email IDs once the minute is generated.

4.10. **Draft Internal Audit Report,**

4.10.1. When the supervisor assigns the internal auditor to prepare Draft Internal Audit report, the IA should have access to all the working papers and audit finding/observation sheet

4.10.2. The system should be able to develop the draft internal audit report. The draft report should be in the following format of **Index-AA**

4.10.3. The report should contain word "Confidential" on the top of the first page of the draft report.

4.10.4. The system should be able to retrieve/generate the name of internal auditor preparing the Draft Report with date and provisional for approval by IA supervisor in the report.

4.10.5. Once the draft report is approved by the IA supervisor, there should be option for the Internal Auditor to send the draft report to the auditee via email ***if he/she is delegated to do so by the IA supervisor.***

4.10.6. The email sent to auditee by Internal auditor should have a link which should take the auditee to a page within the draft report where they can provide their response (Management Response and Management Action Plan) like the one under IA supervisor page. The response and action plan provided by auditee should be in the format of **Annexure V-1** given on page no.94 of Internal Audit Manual. The auditee while preparing the Management Response and Action Plan in **Annexure V-1** should be given the option to save draft, edit the saved response and finally submit the response to the auditor. But the auditee will have no access to the same page once the response is submitted. There should be a pop-up message to confirm to the auditee that submitting the response will be final, hence he/she will not have further access once the response or action plan is submitted.

4.11. **Reporting (MIS)**

4.11.1. The system should provide an option to fill the Reporting checklist by the audit/team leader and head of IAU to make sure that the reporting is completed.

4.11.2. The system should be able to generate and/or upload all the working papers or forms or reports and back-up in the database. Once the reports are finalized, the working papers or forms or reports should not have an option to edit or delete. However, the system should have an option to retrieve any working papers or forms or reports or individual observation/finding with a management action plan.

4.11.3. All the working paper/form/reports should contain the following meta data:

- ✓ Name of Form,
- ✓ Name of Organization,
- ✓ Engagement Name/Audit Topic,
- ✓ File No. and Audit period.
- ✓ Moreover, the working paper/form/reports should contain the person's details who prepared it with the date as well as the provision for the review and approval with the date.

4.12. **Consulting services**

4.12.1. When the internal auditor is assigned by IA supervisor to carry out consulting service, IAMS shall give the right to the Internal Auditors to visit the previous and current year's consulting service documents or report but without editable rights.

4.12.2. The system should automatically generate Consulting Form as per **Index-L** to record the request received from the client and for future references.

4.12.3. The system should be able to record the COI (declare the Conflict of Interest) and able to print if required in the format of **Index CC-1**.

4.12.4. Notify Auditee (an engagement letter).
The internal auditor should be able to generate the Consulting engagement letter. If Consulting service required to go in the field. The engagement letter should be similar to audit engagement but with different subject and contents.

4.12.5. Consulting Observation Sheet
The system should generate a consulting observation sheet like in **Index BB** to record the finding/observation.

4.12.6. Reporting

4.12.6.1. The system should be able to generate all the working papers or forms or reports related to consulting service and back-up in the database. Once the reports are finalized, the working papers or forms or reports should not have an option to edit or delete. However, the system should have an option to retrieve any working papers or forms or reports or individual observation/finding.

4.13. **Monitoring and follow-up,**

4.13.1. The system should have a database for all the observation/finding along with management responses and action plan. There should be an option to indicate/mark in the database when the management has implemented the recommendations.

4.13.2. The IA should be able to search and check the observation of whether the management has implemented the recommendation as per their action plan.

4.13.3. When the recommendations are not implemented then there should have an option to send reminder through email automatically after every 2 months.

4.13.4. The system should also record all the correspondences for future reference.

4.13.5. The system should generate monitoring and follow-up report monthly/quarterly/bi-annually/annually.

5. Head of Agency Homepage.

5.1. Approval of Internal Plan.

5.1.1. IAMS shall have the provision for the head of agency to visit the previous Internal Audit Annual Plan and current year plan.

5.1.2. The option for the approval of the Internal Audit Plan for the Year and/or approval for any amendment of the Internal Audit Plan (inclusion and exclusion of assignments) during the year

5.2. Reports (MIS for IAs):

5.2.1. The system should be able to generate all IA plans and reports (Assurance and Consulting) of the concerned agency through head of agency page. However, the system should permit only viewing and printing options.

5.3. Monitoring and follow-up:

5.3.1. The system should generate the status of implementation of IA recommendations (only for assurance service).

5.3.2. The system should provide an option to search and check the observation whether the management has implemented the recommendation as per their action plan.

5.3.3. When the recommendations are not implemented the head of agency should be able to send reminders through system via email.

5.3.4. The system should generate monitoring and follow-up report monthly/bi-annually/annually/report wise.

5.3.5. The system should also record all the correspondences for future reference.

6. CCA Homepage (Dashboard)

6.1. **Annual Internal Audit Plan:**

6.1.1. The CCA user should have access to entire Internal Audit Unit's Annual Work Plan in the PDF and MS word format with the options to generate individual IAU or group of IAU or ALL annual Internal Audit plans.

6.2. **Reports (MIS for CCA):**

6.2.1. The system should provide access to all the working papers, forms and reports including consulting work in the format of read-only.

6.2.2. The CCA user should also have an option to retrieve any working papers or forms or reports or individual observation/finding with a management action plan and consulting works but without an option to edit or delete.

6.2.3. The system should generate visual reports on audit planned vs executed, categorization of audit findings by priority rating such as critical, high, medium, low, and advisory, coverage of audit against the total budget of the agency.

6.2.3.1. The system should have provision to categories the visual reports in 6.2.3 in the in the following sub-category

6.2.3.2. IAUs: Ministries, Autonomous Agencies and Dzongkhags
6.2.3.3. By fiscal year
6.2.3.4. By similarity of observations
6.2.3.5. By status of recommendations implemented

6.3. **Monitoring and follow-up:**

6.3.1. The CCA user should be able to search and check the observation, whether the individual agency has implemented the recommendation provided by the respective IAU as per their action plan.

6.3.2. When the recommendations are not implemented then there should be an option to send reminder through email automatically after every 2 months to the respective IAU head.

6.3.3. The system should also record all the correspondences for future reference.

6.3.4. The system should generate monitoring and follow-up report monthly/bi-annually/annually/report of individual IAU or group or entire.

6.4. **Annual Internal Audit Report,**

6.4.1. The system should be able to combine all the similar audit observation/finding and consulting works of IAUs and come up with a consolidated IA Annual Report. The report should contain the followings;

- ✓ Uniform Cover Page
- ✓ Table of Content
- ✓ Executive Summary (if the report is more than 5 pages)
- ✓ Main report
  1. Introduction
     1.1. Purpose of the Annual Internal Audit Report
     1.2. The objective of the Annual Internal Audit Report
     1.3. Scope of the Annual Internal Audit Report
     1.4. Methodology or Approach
     1.5. Limitations
  2. Background
  3. Key observations and recommendation (There should be option to add, edit or delate the key observations and recommendation). For example:
     3.1. Observation 1
     3.1.1. Action taken and Improved the system
     3.2. Observation 2
     3.2.1. Action taken and Improved the system
  4. Conclusion.

7. PMO officials Homepage

7.1. PMO officials Homepage shall have the provision/option for the PMO officials to view entire Internal Audit Unit's previous Internal Audit Annual Plan and current year plan. However, the system should permit only viewing and printing.

7.2. **Reports;**

7.2.1. The system should be able to generate entire IA plans, reports (both assurance and consulting) and CCA Annual Report. However, the system should permit only viewing and printing.

7.3. **Monitoring and follow-up;**

7.3.1. The system should generate the status of implementation of IA recommendations.

7.3.2. The system should generate monitoring and follow-up report monthly/bi-annually/annually/report wise.

7.3.3. The system should provide an option to search and check the observation whether the management has implemented the recommendation as per their action plan.

7.3.4. When the recommendations are not implemented, there should be an option to send reminder through email.

7.3.5. The system should also record all the correspondences for future reference.

8. Audit trail.

8.1. The IAMS system should have an option to record all the working (audit trails) once the system is rolled out.

8.2. **Administrator rights:**

8.2.1. The systems should provide an option to the administrator for resubmission of reports by the users.

8.3. **User Manual**

8.3.1. The Developer shall develop a user manual for Internal Auditors and managements to use IAMS.

8.3.2. The User Manual should capture all the process in IAMS such as;

- ✓ Registration of all user
- ✓ Internal Audit planning (Including all the process)
- ✓ Internal Audit Engagement (Including all the process)
- ✓ Preparation and submission of Internal Audit Reports (Including all the process)
- ✓ Monitoring and Follow-up (Including all the process)

9. Training

9.1. **Developer shall**:

9.1.1. Train all the Internal Auditors fully in IAMS.

9.1.2. Propose training duration which should not exceed one week per batch.

9.1.3. Prepare training contents and course deliverables

9.2. **CCA shall**:

9.2.1. Identify Trainees

9.2.2. Arrange logistics such as venue, refreshment, working lunch, training materials such charts, marker pen, whiteboard and etc

9.2.3. Process Developer Trainers Permits and VISA (if required)

9.2.4. Facilitate the training program

10. Technical Requirements

Note: *Following provisions have been prepared for both: COTS or BESPOKE applications. Provisions not applicable in either approach may be ignored*

10.1. General Requirements

10.1.1. The proposed IAMS shall comply/adhere to following technical requirements/functionalities, but not limited to:

10.1.2. Use Responsive Web Design technologies, (HTML 5, CSS3)

10.1.3. Implement data validation for both client and server (eg: AJAX technologies, JavaScript, etc).

10.1.4. Implement Search, Save, Create, Read, Update, Delete (SCRUD) operations and auto save if the users are idle for 60 seconds.

10.1.5. Maintain consistent aesthetics and UI of the software;

10.1.6. Ensure compatibility to all the browsers (Mozilla Firefox, Internet Explorer, Google Chrome, Opera, Safari, etc.);

10.1.7. The IAMS should be scalable and upgradeable as and when the number of users and contents increases; Up to 100 IA User, 50 supervisor user, 50 management user and 10 CCA user and 5 PMO officials user transactions per year with provision of increment annually.

10.1.8. Maintain and ensure that the web-based software system supports minimum up to 50 concurrent users;

10.1.9. The IAMS should have provision to support English and Dzongkha. This requirement can be provisioned both from front-end APIs and backend database system design by incorporating appropriate UTF based locale support.

10.1.10. The IAMS shall have status bar to guide user step by step to use the system (e.g during registration, stage of registration to guide by status bar).

10.1.11. The IAMS shall have capability to notify via Email wherever there is a system disruption or maintenance either to specific group or individual.

10.2. System Performance, Availability and Reliability

10.2.1. The maximum response time for the system shall not exceed 15 seconds 95% of the time on a PC connected to a network with minimum bandwidth of 512 kbps. The bidders shall develop the necessary test programs to verify the response time. All necessary testing tools required for such performance testing shall be provided by the bidders for the purpose of the testing at no additional cost to the client. The availability of the system can be recommended by developer.

10.2.2. The scheduled operating hours for the system shall be twenty-four hours a day, seven days a week, including Sundays and public holidays.

10.2.3. The developer shall state any scheduled downtime required but limited to only 3-4 rounds of scheduled downtime a year for maintenance unless approved by clients. The downtime shall be scheduled up to 3HRs and planned on non-working hours.

10.2.4. The Developer shall ensure the reliability of the System by incorporating the following features: Failure of any transaction shall not affect integrity of the data captured/stored in the System.

10.2.5. Failure of a transaction at a workstation or an internet session shall not affect users at other workstations or internet sessions. The effect of a failed transaction on the database shall be automatically and dynamically backed up and recorded.

10.2.6. The System shall be able to recover all data stored up to the last completed transaction before a system failure occurs.

10.2.7. The Developer shall ensure that any rectification, enhancement or change to the System shall not affect its system reliability

10.3. Security Requirements

10.3.1. The components of the IAMS are responsible for maintaining security to meet Confidentiality, Integrity and Availability requirements

10.3.2. The IAMS shall comply Information Management and Security Policy (IMSP) during deployment.

10.3.3. To ensure confidentiality and integrity of the System, the bidder shall propose solutions to protect the data from being accessed, altered, or deleted without proper authorization.

10.3.4. The IAMS shall maintain time series data so that information is not lost with passage of time and repeated updating.

10.3.5. The IAMS shall have up-to-date CAPTCHA program as a remedy to stop spam and other intrusions wherever required.

10.3.6. The forms shall have Input validation to prevent attacks such as buffer overflows, cross- site scripting, SQL Injection.

10.4. System Security

10.4.1. The bidders shall minimally provide Access control, Authentication, and accountability security mechanisms for backend operations of the System.

10.4.2. The security solution proposed shall be scalable but not affect the performance by creating a bottleneck or single point of failure to the overall system.

10.4.3. The system should provide tamper-proof audit trails and logs for administrator or auditor to check for the actions committed by users. The audit trails shall consist of following details but not limited to:

- ✓ Login and logout
- ✓ Attempts to access unauthorized resources
- ✓ User profile changes
- ✓ Past audit events.
- ✓ Track all actions performed on documents attached/uploaded.

10.4.4. The system should have provision to assign the access rights of other resources on need basis to authorized users.

10.4.5. Information in the System that is deemed to be sensitive shall be encrypted and protected from accidental and/or unauthorized modification.

10.4.6. The System shall provide automatic session disconnection for inactive user after session time [Proposed best practice session time] is over.

10.4.7. The system shall protect the audit trails from being modified by unauthorized personnel or privileged users.

10.5. Access Control

10.5.1. The access to the different modules within the System shall be via a common logon. The bidder shall propose an efficient, faster and easier login page for the users.

10.5.2. The system shall have provision for the management of access rights for the user either individual or group level.

10.6. Recommended Development Platform:

10.6.1. The developer shall comply with the Electronic Government Interoperability Framework (e-GIF) during the development of IAMS for customized solution.

10.6.2. The IAMS system development is recommended to be implemented using Open Source Languages framework based on Java, PHP, Ruby, etc.

10.6.3. The application is recommended to be implemented using MVC (Model View Controller) based web frameworks, address protocols and standards including application security and manageability. If the developer has alternative development proposal, developer may provide the details on the proposed language

10.6.4. The database for the application is recommended to be implemented using Open Source Database such as MySQL, PostgreSQL, etc.

10.6.5. The consultant shall comply with e-GIF Data standards such as Table naming conventions, data modeling, data types, codes, etc. during the customization of IAMS.

10.7. Development/Customization Methodology:

10.7.1. Modular based approach and Agile SCRUM methodology must be used for the design and customization of the IAMS to ensure all requirements and feedbacks of the client are identified and incorporated.

10.7.2. Bidder may provide once in two weeks updates to clients (functional features, presentation of views, demos, etc. of the portal). Bidder may recommend suitable reporting period based on their best practices.

10.7.3. Bidders may carry out at least 2 iterations of requirement or specification reviews for each sprint before implementation of next module from the product backlog

Indexes to appendix II