TERMS OF REFERENCE (TOR)

Advisory Support for the IT Audit of PFM Information Systems

DEPARTMENT OF PUBLIC ACCOUNTS

MINISTRY OF FINANCE, ROYAL GOVERNMENT OF BHUTAN

Contents

TERMS OF REFERENCE (TOR)

Advisory Support for the IT Audit of PFM Information Systems

1. Project Background

The Financial Management (FM) Systems in Bhutan have come a long way from manual intervention to real time online systems. Ministry of Finance (MoF) has established strong in-house software development, help desk, system management and maintenance capabilities to provide effective technical support for key business requirements mainly related with the public expenditure management, accounting and reporting functions since early 2000. The digital transformation has not been very smooth considering the poor network connectivity and the lack of ICT expertise.

With the initiative and implementation of **GOVNET** (TWAN, DZONGKHAG WAN, Thromde WAN) and **Government Data Centre** (GDC) by Department of Information Technology and Telecom (DITT) under the Ministry of Information and Communication, the network connectivity has significantly improved, making online systems easily accessible. Data Hub, an important initiative of DITT developed for/on a Whole-of-Government Data Exchange platform allows the authoritative Data/Information Asset to be shared and reused seamlessly making it possible for the systems to be integrated, using API (Application Program Interface).

The current FM systems under Ministry of Finance were developed to mainly manage or standardize each individual Organization's procedures, to record data and to provide faster services. The list of FM Systems in Bhutan, particularly under the Ministry of Finance are as follows: -

1. Multi Year Rolling Budget System (MYRB - online) owned by Department of National Budget developed on .NET and MS SQL 2016 - operational since 2010, caters to 200+ users (Government to Government). Certain transparency and efficiency in budget allocation and monitoring has been enhanced with this system. The major reform that we are looking forward to is in decentralizing the budget process and delegating responsibilities from the central budget agency to individual agencies and also introducing monitoring and evaluation measures as part of budgeting process.

2. Public Expenditure and Management System (PEMS - online) owned by Department of Public Accounts developed on .NET and MS SQL 2016 - operational since 2010, caters to 750+ users (Government to Government). This is one of the main information systems of MoF, used for public expenditure management, accounting and reporting needs. Most of the entire process of government financial transactions has been digitalized expect for electronic payment, which is developed in-housed and will be rolled out in the next financial year (2019 – 2020). With ePayment process in place, the cheque payment will be replaced by electronic fund transfer and the account reconciliation would also be on a real time basis.

3. Revenue and Administration Management System (RAMIS- online) owned Department of Revenue and Customs developed on JAVA and MySQL – operational since 2016, caters to 10,000+ users (Government to Government, Government to Businesses and Government

to Citizens). This is a tax administration system that has been developed to automate manual tax filing, monitor taxes and to generate reports related to taxes. By 2022, RAMIS will be replaced by a robust, online system called Bhutan Integrated Tax Solution which will have Revenue, Tax, non-Tax and Sales (all in one) modules together in one system.

4. Bhutan Automated Customs System (BACS) also owned by the Department of Revenue and Customs developed on JAVA and MySQL is a standalone system that caters to both imports and exports. It is one of the oldest systems in the Ministry of Finance which will soon be replaced by CMS (Customs Management System), an online system which is currently in a conceptual phase and will include a risk management module too.

5. Electronic Government Procurement System (eGP – Online) owned by the Department of National Properties is a customized off the shelf digitalized procurement system where in the manual procurement procedure has been streamlined to maximize effectiveness, efficiency and transparency.

6. Asset Inventory Management System (AIMS – Online) also owned by the Department of National Properties, developed on JAVA and MySQL – operational since 2017, caters to 1000+ users (Government to Government) is an Asset Inventory Management System, where all the assets, once procured through eGP needs to be recorded and monitored to curb corruption and misuse.

7. Commonwealth Secretariat Debt Recording Management System (CS-DRMS) used by the Department of Macro Economics is a commonwealth Secretariat off the shelf product used since 2006 for debt recording and management.

All the above systems except for CS-DRMS and BACS are hosted in the Government Data Center (GDC) at the IT Park, Thimphu with the disaster recovery (DR) site coming up soon at Bumthang, central Bhutan.

MoF with the help of the World Bank, strives to bring about further improvements in the PFM framework and systems by strengthening and integrating stand-alone PFM information systems into an Integrated Financial Management Information System (IFMIS) and establishing data warehousing with Business Intelligence tools and mining capabilities.

For the PFM systems to expand and accommodate IFMIS, network connectivity, information security and Data Center operation needs to be assessed and improved/upgraded. In order to have an integrated web based system that provides real time analysis on government's fiscal activities including budget formulation, execution, account settlement, Payroll management and performance management/monitoring, the FM systems under MoF needs to be integrated with other relevant systems like HR information system (Royal Civil Service Commission) to have proper payroll control mechanisms in place; Audit Regulatory and Management System (Royal Audit Authority) to validate the accuracy of the reports, Government Performance Management System (GPMS) to monitor the performance of the Agencies and the Planning and Monitoring Evaluation System (PLaMS) to sync/monitor annual activities with the planned activities .

With ePayment in place, PEMS has been enhanced to facilitate online transactions in order to have efficient real time bank reconciliation and cash management control. Payroll has also been enhanced to efficiently disburse the salary and remittances on time. Following APIs have been developed to;

1. Integrate PEMS with RAMIS, for fetching the tax information details (Vendors and Employees) and to automatically upload the TDS (Tax Deducted at the Source) and the Revenue Remittances details to RAMIS, without the users of the PEMS having to log into RAMIS to upload the details via Data Hub;
2. Integrate PEMS with BOBL (Bank of Bhutan) for payment settlement;
3. Validate the payee account number maintained at the banks;

In line with above system enhancement and integrations, MoF deems it necessary to perform a comprehensive Technical Audit of the current Financial Management Systems under Ministry of Finance (MoF), its integration modules involving the stakeholders and their respective systems, ICT infrastructure and technical practices. The systems should be thoroughly assessed to identify the current processes, the future state integrated processes for the move towards Integrated Financial Management System (IFMIS) and develop a strategy to address the gaps. This is to ensure that the system is thoroughly assessed and all issues ranging from network connectivity, change management, business process management, system architecture, design and especially system security are identified, and resolutions implemented prior to the roll out of the Additional Financing Project.

2. Objective of the IT Audit

The objectives of this IT Audit are to:

- Provide management with an independent assessment of efficiency and effectiveness of the design and operation of internal controls and operating procedures and the identification of application-related issues that require attention;
- Provide management with an evaluation of the IT function's preparedness in the event of a process disruption , identify issues that may limit interim business processing and restoration of same and provide management with an independent assessment relating to the effectiveness of the IT continuity plan and its alignment with the business continuity plan and IT security policy;
- Provide management with an assessment of the effectiveness of the information security management function; evaluate the scope of the information security management organization and determine whether essential security functions are being addressed effectively;
- Provide management with an independent assessment relating to the effectiveness of the network perimeter security and its alignment with the IT security architecture and policy; provide management with an evaluation of the IT function's preparedness in the event of an intrusion and identify issues that affect the security of the enterprise's network;
- Perform a review of the change management process to provide management with assurance that the process is controlled, monitored and is in compliance with good practices.
- Review of the IT Infrastructure and organisation in terms of technology and capacity to handle current and planned activities as well as physical and environmental controls at the data centers;

- Perform a review of current network connectivity and provide management with an assessment of opening up the current network to the Internet. This will include the implications of an open network, potential architecture, security as well as business processes.

The Consulting Firm (the Consultant) is expected to produce an assessment report based on one of the acceptable frameworks (e.g. CobiT[1]) and suggest possible improvements in ICT strategy and governance model and develop an action plan for implementation of suggested improvements.

3. Scope of Work

The Information Systems Audit should practically and systematically support the following logical audit functions:

3.1 Audit Plan

The Consultant shall conduct an IT risk assessment and present its findings in a formal workshop to secure consensus among the Ministry's stakeholders. The purpose of the workshop is to ensure that the Ministry has suitable input into completion of the assessment. The workshop shall be concluded with a risk-based IT Audit program along with the relevant detailed solutions and their related supervision tasks. The Plan shall cover but not limited to the following topics:

- Review a vision and a mission statement for the Information Technology Unit;
- Offers a general objective assessment of the Ministry's Information Technology environment in terms of staff, equipment and architecture;
- Review and recommend current technical architecture (e.g. applications, data, technology and network connectivity etc.);
- Review and complement effective policies, standards and procedures for IT governance and related decision making;
- Propose an established framework (like CoBIT) for the assessment of all controls;
- List of audit activities subject to approval by the Ministry
- Review and recommend effective change management procedures; and
- Provide an implementation plan with an estimated timeline.

The most obvious source of Best Practice for information security is ISO, the coordinating body for most of the world's national standards bodies. For example, ISO/IEC 27002, the Code of Practice for Information Security Management, is part of a coherent and growing suite of information security standards (the ISO27k series) that is being actively developed and extended. The consultant is expected to use well defined standards like CoBIT (all controls included in the latest version) and ISO27k series during this assessment.

[1] Control Objectives for Information and related Technology (COBIT) (www.isaca.org/cobit).

3.2 Audit Detailed Activities

Within the context of the plan's total management solution, the functions of the Audit shall include but not limited to the following activities:

a) Security Assessment — To Ensure that security is built into the application: Verify custom security requirements, privacy requirements, security coding best practices, security application design rules, and security testing benchmarks. Also review the systems infrastructure by examining the enterprise wide systems (Servers, Storage, Windows, and LANs etc.)

b) Inputs, Processing, Outputs: Verify evidence of data preparation procedures, reconciliation processes, and handling requirements. The auditor must obtain evidence of adequate control over manual processes such as user data preparation procedures are in place. It is essential that manual inputs are completed and appropriately authorized prior to being processed by the systems. The auditor must review business processes around transactions initiation and their system entry points.

c) Administration: It is essential to verify, if systems ownership, custodianship and responsibilities are clearly established and if Controls are in place to ensure that segregation of duties exists between business owners, developers, and operational support.

d) Change Request Procedures: Verify that an effective Change Request Procedures system is in place and that all changes are documented, whether they are break fixes, enhancements, or major revisions (releases). It is essential that any change to the application is first initiated by a request that is reviewed and approved by the appropriate associates. The documentation around the Change Request Procedures process needs to specifically call out who can request changes, who can approve changes, and who can move these changes into production. The auditor should confirm the segregation of the three roles and report any discrepancies in this regard.

e) Source Code Analysis — To Verify that security is Implemented in the Code: Assesses stability and security of code i.e. authentication, authorization, logging, versioning and input validation.

f) System Penetration Testing: Two levels of system penetration testing are required:

- Verify whether the application is vulnerable to common attacks, a basic system penetration testing, which simulates the types of attacks that could be launched on the systems
- Verify whether the systems are vulnerable to unique attacks (such as attacks on systems logic), design and execute system penetration tests that attempt to subvert the system's security mechanism.

g) Systems and Applications: Verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity

h) Information Processing Facilities: Verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions

i) Systems Development: Verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development

j) Management of IT and Enterprise Architecture: Verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing

k) Telecommunications, Intranets, and Extranets: Verify that controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers

l) Runtime Analysis — To Expose Buffer Overflows: Perform tests to pinpoint most possibilities for memory corruption and leaks, and then present the findings along with the appropriate corrective measures

m) Provide a Risk Score: Design a quantitative score for the risk associated with the audited systems and databases

n) Develop a Security Policy: Develop appropriate security policy to close the gaps arising from the Information Systems Audit

3.3 Modules Covered Audit

The following is the list of modules to be covered by the auditors within the scope of this assignment:

Key MoF information systems to be reviewed during this assignment include:

1. PEMS
    1. Financials Core Transactions
        a. General Ledger
        b. Accounts Payable
        c. Accounts Receivable
        d. Cash Management
        e. Business Process Management
        f. Service Connect Runtime
        g. Payroll Control / Management
    2. Advanced Financial Report Viewer
    3. Multi-Site Management
    4. Interface with the Banks/GIFT
    5. Interface with RAMIS

6. Interface with CSIS – Civil Service Information System of RCSC
9. Replication Server License
10. Advanced Financial Report Designer

2. CSDRMS (debt management system) interface
   a. Cash and debt management

3. Asset Inventory Management System

4. Procurement Management System
   a) Commitment control in the multiyear investment

5. MYRB
   a) Active Planner (Budget Preparation)
   b) Budget execution reports
   c) Interface with PEMS

6. eGP – electronic Government Procurement

7. AIM – Asset Inventory Management

Other platforms/capabilities that should be included in this review include:

- User Access
- SQL Audit Trail
- Data Retention/Storage/ Archive
- Reports (development and retrieval)
- Business Continuity solutions

Several other MoF information systems and technical capabilities can be added to above lists after the initial review of PEMS and MYRB by the consultants.

4. Deliverables and Reporting

The following is a list of expected deliverables:

- An inception report including the details of the proposed audit plan to be presented in a workshop for MoF staff. (1 Weeks)
- Draft final report including items listed below: (4weeks)
  a. Systems Audit report
  b. IT Risk Assessment Report
  c. Security Policy
  d. Gap analysis for International standards compliance (ISO 2700x, CoBiT)
  e. Recommendation of corrective activities along with their implementation schedule
  f. Specific recommendations on possible network architecture and security policies on opening up the current network to the Internet.
- Final report after draft report being reviewed by the Ministry of Finance (6 weeks)

The Reports shall contain the standards verified, deviations, if any, the adequacy of standards and the adherence to the envisaged standards by the Ministry of Finance. The reports should be discussed and agreed with the Ministry of Finance governance committees and should be structured in a manner giving the observations, the implications of the findings, the suggested recommendation and the management comments / agreed actions. In addition, the Information Technology Systems auditor should provide an **Executive Summary** highlighting the critical issues, which require the attention of the Ministry of Finance, and their mitigation plans.

4.1 Payment Terms

Sl.No	Description	Percentage
1	Submission and acceptance of inception report	20%
2	Submission and acceptance of Final CoBIT report for Bhutan	80%

5. Implementation Arrangements

The audit will be implemented in the main offices of the Ministry of Finance. The Ministry of Finance will make all logistics available. The contractor should be given access to all systems and legal documents, correspondence, books of accounts, Financial management reports and any other information as deemed necessary for the project.

Access to view relevant systems of the stakeholders' should be given on prior approval from the concerned management.

6. Period of Appointment

The Consultant would be appointed for a period of **six weeks of onsite work** and cover the activities listed in this ToR. The input expected from two experts during this period is around 60 person-days. The assignment shall commence as soon as practical, and be completed within a period of two months.

7. Qualifications

The Consultant should be experienced in conducting independent IT audit. The Consultant team will consist of two ICT Auditors to perform the activities highlighted in this ToR. The Consultant (Consulting Firm) will have the following qualifications:

1. At least ten years of consulting experience in similar ICT assessments and audit assignments.
2. Substantial project management and organizational change expertise. Proven proficiency in the preparation of study reports and ability to communicate project issues with high

ranking officials, and to resolve key issues quickly. Proficiency in one or more Project management standards (PMBOK, Prince2) is required.

3. Expertise in managing large public sector ICT projects especially in the field of public financial management systems will be an advantage.
4. Strong skills and knowledge of international standards and control frameworks including CobiT, ITIL and ISO 2700x will be essential.
5. Fluency in English is required for all members of the team.
6. Excellent report-writing and human relations skills.

The **Team Leader** shall possess the following qualifications:

1. At least seven years' experience of information systems audit in corporate or public sector. Hands on experience of risk management.
2. Master's degree (or University degree and demonstrated experience) in informatics, engineering or related fields.
3. ICT Audit qualification (Certified Information Systems Auditor or equivalent).

The **IT Auditor/s** shall possess the following qualifications:

1. At least five years' experience of ICT Audit in corporate or public sector.
2. University degree in informatics, engineering or related fields;
3. ICT Audit qualification (Certified Information Systems Auditor or equivalent).

The qualifications of the selected Consultant have to be satisfactory to the World Bank.

7.1 Criteria, sub-criteria, and point system for the evaluation of the Proposals:

Criteria	***Points***
(i) **Specific experience of the Consultant (as a firm) relevant to the Assignment:**	*45*
(ii) **Adequacy and quality of the proposed methodology in responding to the Terms of Reference (TORs):**	*20*
(iii) **Key Experts' qualifications and competence for the Assignment:** *a) Team Leader* *[20]* *b) IT Auditor* *[15]*	
Total points for criterion (iii):	*35*

The number of points to be assigned to each of the above positions shall be determined considering the following three sub-criteria and relevant percentage weights:

1) General qualifications (general education, training, and experience): 25%

2) Adequacy for the Assignment (relevant education, training, experience in the sector/similar assignments)*:* 75%

Total weight: 100%

Total points for the three criteria*:* 100

The minimum technical score required to pass is*:* 70

8. Special Terms and Conditions

8.1 Location of Work

The work will be carried out in Thimphu, Department of Public Accounts

8.2 Reporting Arrangements

The Consultant will work under the supervision of Ms Karma Yangkee, Chief ICT Officer, Ministry of Finance

8.3 Administrative Information

- The bid price will include taxes with clear line for VAT. The Consultant will include a breakdown of their price, in terms of the inputs from two experts (person-days) and unit rates, and the details of reimbursable cost items listed below.
- Reimbursable items include international travel and accommodation in Thimphu.
- Per diems will be paid for all working days at the rate applicable at the time of request.

The Consultant shall be fully responsible for providing his staff with the requisite equipment and resources, to enable them to concentrate fully on their assignment.

9. Restrictions

In addition to the standard conflict of interest restrictions specified in the consulting contract, all materials created under this Contract will remain the sole property of the Ministry of Finance of Bhutan (MoF). Re-use of the materials will require the formal, written approval of the MoF.

The Consultant shall have no material interest in any of the outputs of this assignments and technologies or related ICT services under consideration, and will not be eligible to participate in future contracts for the implementation of the IFMIS.

On the commencement of the assignment, the Consultant will jointly prepare with the MoF a statement of confidentiality that will bind the Consultant to nondisclosure of any sensitive information that the Consultant may become knowledgeable of during the course of the assignment. The terms of this agreement shall be made consistent with the relevant privacy laws of Bhutan.

10. Selection

The Consultant (Consulting Firm) will be selected under the provisions of the World Bank's Guidelines for the Selection and Employment of Consultants, July 2016 Edition, revised in October 2017, based on the method of Consultant's Qualifications (CQS) and a Lump-Sum Contract (payments linked to deliverables) will be signed.