Term of Reference

of consulting service for conducting IT Security Audit of FCGO IT Systems

1. Background:

Financial Comptroller General Office (FCGO), an organization under the Ministry of Finance (MoF), is the main agency responsible for the Public Financial Management (PFM) system of Government of Nepal (GoN). The treasury operation is the pivotal function of this office as the central level function. In order to manage the treasury, it also carries out the functions mentioned in the Financial Procedure Act, 2055 (B.S.) and Financial Procedure Regulation, 2064 for this office. Actually these laws for this office have mandated the major functions. As per the said law this office mainly oversees budget implementation, treasury administration, internal audit, budget expenditure implementation, cash and budget management, expenditure and revenue accounting, expenditure and revenue tracking, other receipts management, human resource management, strengthening the accounting system and preparation of consolidated financial statements of the government.

There are District Treasury Comptroller Offices (DTCOs) in 75 districts under this office. In Kathmandu district there are additional four TSA counters. The DTCOs release the budget and manage the fund for the expenditure and control the accounts for the offices operating under the line ministries of GoN.

FCGO has been investing on IT at its top since more than decades for the achievement of a complete e-governance system. The organization to some extent is on the way to success through the development and implementation of few software systems for the management and treasury operations.

PFM system of GoN can be visualized as the most vital and critical responsibility of civil servants as it is concerned with the management of public finance. The improvement in ICT to form an e-governance system will adds on the improvement of PFM system. The systematic management of finance through IT will certainly result on real time, accurate, versatile and transparent information.

Presently, FCGO is engaged in the development and up gradation of web-based IT Systems:

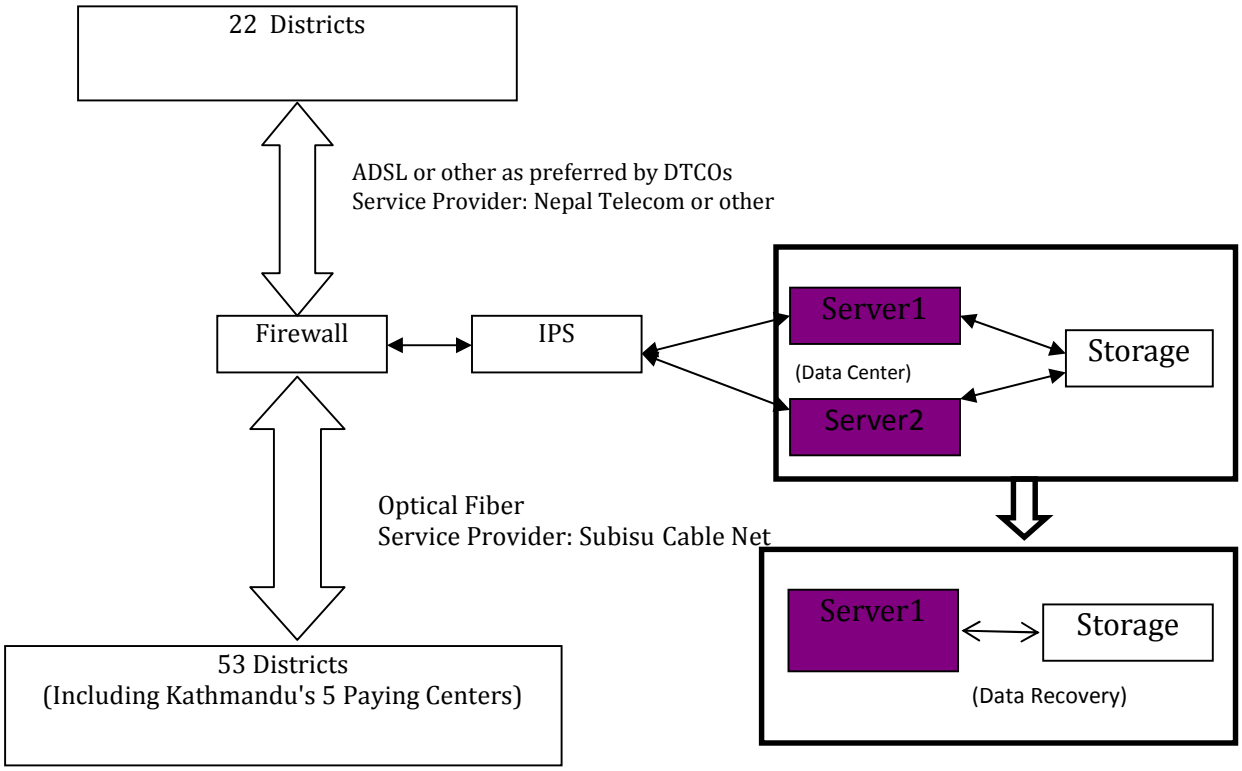
- **Treasury Single Account – District Expenditure Control System (TSA-DECS):** The application is centralized and is developed in Oracle Forms and Reports 10g with Oracle database 11g. TSA DECS is used by all districts for managing budget expenditure, revenue and retention money of Paying Offices of the district and the support required for its operation is provided by FCGO.
- **Financial Management Information System (FMIS):** This system developed with Oracle Forms & Reports 10g and Oracle Database 11g and is used for compiling entire data of budget release, expenditure, balances, virement, revenue collection, retention money from TSA. The FMIS gives consolidated information regarding entire financial performance of the districts obtained from DTCOs. FMIS is the means by which the FCGO exercises control over the DTCOs and ensures that data is accurate, complete and well timed. It is the main source of reporting of the budget execution, revenue collection and retention money. FCGO produces different financial reports at different intervals using such data.

- **Revenue Management Information System (RMIS)**: The system is developed with Oracle Forms & Reports 10g and Oracle Database 11g. RMIS is the application for recording the collection of revenue and is implemented in 50 districts. In parallel, RMIS for diplomat is also developed and being updated with its implementation in …. Countries. This application is developed with Oracle APEX and Oracle Database 11g as backend.
- **Computerized Government Accounting System** (**CGAS)**: CGAS records every financial transaction of the government ministries, departments, offices, projects and generates financial reports as and when required. Presently, the system is being developed with complete provision of recording operation level expenditure at government's ministries, departments, offices and projects with customized reporting system.
- **Other Systems :** Debt Management System, Investment Management System, Treasure Management System, Budget Management System, Reimbursement Management System, Public Assets Information Management System etcs.

Application environment: Most of these Systems have been developed using **Oracle 11g** database as backend, Oracle application server as middle tire and **Oracle forms & reports 10g** as application development platform. Servers in FCGO are AIX6.1. Nepali Unicode is used for the nepali text in the

system and the database. Clients need to be installed with Java 6 in any OS. Client machines are currently using Windows machines for operation.

System Architecture



FCGO is responsible for smooth and consistent operation and maintenance of mentioned IT System. Moreover, FCGO intends to perform Security audit of its IT infrastructure to analyze the gap (if exist) and ensure the security.

2. Purpose and Objectives:

The Purpose of IT security audit is to provide an independent evaluation of Application, Database, Server Architecture and Network infrastructure to identify any gaps between the FCGO systems and an adequate IT security framework as well as Nepal government's Enterprise Architecture **(NeGEA)** Framework.

3. Scope of IT Security Audit:

The scope would include assessment of FCGO applications, security devices, server, Network and associated IT infrastructure.

4. Responsibilities to be performed by Consultants:

A comprehensive Information Systems Security Audit must be undertaken covering the various key processes and procedures undertaken at the following two locations / sites:-

1. Financial Comptroller General Office (FCGO), Anamnagar
2. FCGO's DR system at GIDC, Singhadurbar
3. One District Treasury Controller General, Office (DTCO will be selected by FCGO)

The audit/assessment will be carried out using CMM (Capability Maturity Model) methodology against ISO 27001 ISMS.

The Audit at the two locations shall include, but not be limited, to the following:-

1. Operating System (OS) for servers, Databases and other Installed systems

a. Set up and maintenance of system parameters
b. Patch Management
c. Change Management Procedures
d. Logical Access Controls
e. User Management and Security
f. OS Hardening
g. Performance, Scalability and Availability
h. Consistency with requirement Specification

2. IT Processes and IT Management Tools from security point of view

a. IT Asset Management
b. Enterprise Management System
c. Help Desk
d. Change Management
e. Incident Management
f. Network Management
g. Backup & Media Management
h. Enterprise Anti-Virus Management
i. Vendor & SLA Management

3. Security and Privacy Management

a. Security & Privacy Policies
b. Penetration testing and Vulnerability Assessment (PT / VA) of various security zones.

4. **Application Audit:**
    a. Application Functionality Audit
    b. Application Security Audit
    c. Convenience and Efficiency in system use
    d. Compliance with GEA Framework
    e. Software Document Management
    f. Change Management
    g. Scale Management
    h. Operating Manual Management

5. **Database Design and Administration:** The consultant is required to verify the standard of database structure and its proper administration (Regarding Backup and Restore policy) from security point of view.
6. **Network**
    a. Network architecture review from security point of view
    b. Network traffic analysis
    c. Virtual LANS (VLANs)
7. **Review the existing IT related policy/procedure documents of the FCGO and suggest required changes.**

5. **Availability of Documents:**

The use of Participatory process requires the consultant will be expected to provide for active and meaningful engagement of relevant government representatives and other stakeholders. The relevant documents may include:

- Requirement Specification and Technical Specification of the OS, Database, developed applications and other installed system.
- Document Presenting Existing IT Scenario including Hardware, Software and Networking.
- Nepal GEA Guidelines.

Beside these, other relevant documents require for the assessment will be certainly made available.

6. Consulting Firm Qualification and Experience

The consulting firm should have the following qualifications and experience to carry out the work

- Company/Firm/Business registration certificate.
- VAT and PAN registration
- Tax clearance certification.

Experience of the consulting firm

- **General experience**: The Consulting Firm must have 10 Years of Experience in the field of IT consulting service/application development.
- **Special Experience as advantage**: Firm having experience of Information system security audit of Public sector.

7. Qualification and Experience of Manpower

7.1 Team Leader (One-13 weeks)

At least Master degree in Information Science, Computer Engineering or Equivalent.

General Experience: At least 10 years of experience in the field of Information system audit.

Specific Experience: At least 5 years of experience of leading ISS Audit.

7.2 Finance Expert (One-5 weeks):

At least Master degree in Finance or equivalent.

General Experience: At least 10 years of experience in Public Financial Management sector.

7.3 IT Expert (Two-13 weeks)

At least Bachelor in computer Engineering, Computer Application or Equivalent with Certified Information System Security Professional (CISSP).

General Experience: At least 5 years of experience in the field of Information System Security Audit.

Specific: Experience of min 2 IT audits (with 1 ISS Audit) of comparable size and complexity in Private/Public or government Organization is Preferable.

(The firm can provide additional assistants (if required))

8. **Evaluation Criteria:** The evaluation criteria for evaluation of the proposal will be as mentioned below.
   - Experience of Consulting Firm
     - General Experience
     - Special Experience
   - Qualification and Experience of Manpower
     - Team Leader
     - Finance Expert
     - IT Expert
   - Methodology of Job accomplishment and work plan
   - Knowledge Transfer
   - Understanding of TOR

9. **Duration of Services:**

   The consultant should perform and submit the Report in no more than 12 weeks from the date of agreement. FCGO as a first party will provide all relevant documents and information on time.

10. **Procurement Methodology:**

    The selection method will be Consultant's Qualification selection (CQS) method as per World Bank procurement Guidelines.

11. **Deliverables:**

    The consultants are required to provide following deliverables:

    - Inception Report
    - Draft Gap Analysis Report, with recommendations, and
    - Final Report along with various reports of scripting and VAPT tools

12. **Payment Schedule:**

    20 % of Total contract price after acceptance of inspection reports

30 % of Total contract price after acceptance of draft reports

50 % of Total contract price after acceptance of final reports

13. Presentation:

The Consultant should present the final draft of the 'IT Security Audit of FCGO IT System' in detail in FCGO. S/He may also require being involved in group discussion regarding the preparation, modification and final submission of Audit Reports.