Terms of Reference

Procuring a Consultancy Firm for Revamping the Government Information Center (GIC) Portal and the Development of the GIC Mobile Application

ICTA/GOSL/CON/QCBS/2017/25

1. Introduction;

The Re-engineering Government Programme (Re-Gov) has initiated number of projects enabling the increased efficiency of the citizen service delivery mechanism of the government. During the identification of the potential development areas, the Re-Gov programme has recognized various difficulties faced by the citizens in obtaining information over the services provided through numerous government organizations. In facilitating the need, the GIC – Call Centre project has been launched and as the online version of the call centre project, the GIC portal www.gic.gov.lk was successfully completed in year 2009.

The GIC portal contains the information of more than 300 government organizations which are broadly categorized into government ministries, departments, statutory bodies, government banks, government hospitals, provincial councils, district & divisional secretariats and local government authorities. It further provides information related to services provided through the aforementioned government organizations with an organization level categorization.

2. Background;

In order to rapidly innovate and remain competitive within the society, any ICT system shall be structured in a way that it caters the practical requirements of the target audiences at different stages. Moving inline with the observations over the GIC portal usage statistics, it has been recognized that, the current information arrangement approach of the GIC web portal is more organization and service centric, where the actual call from the citizens is for an intention based approach, that the service information could be captured in no-time with a great level of accuracy and satisfaction.

Further it has been identified that the information published at the Government Web Portal – www.gov.lk, GIC portal and the GIC knowledge base is similar in nature with different presentation arrangements. The content repetition and the mismatches due to unsynchronized content update practices followed by the government organizations with the current setup, has caused the web portals a less reliable source of information to the citizens. Further, the necessity of exposing the same government information via a mobile application, giving high priority to the application usability, considering the local mobile application usage patterns, has been identified as another major initiative, which will add as an alternative access channel to government service information.

While resolving the downsides of the existing setup and keeping the country in line with the International information sharing standards, ICTA intends to carry out revamping of the Government Information Center Portal and the development of the Government Information Center

Mobile Application, with a centralized and steady information access framework, facilitated via Application Programming Interfaces (APIs). It is expected to incorporate the most modern communication methodologies used around the world with a success note, that will further comes in as a value addition to this national level effort.

3. Concise statement of the objectives;

ICTA intends to procure and obtain the services of a consultancy firm to carry out revamping of the Government Information Center Portal and the development of the Government Information Center Mobile Application. During the assignment, the consultancy firm is required to conduct a detailed requirement study, research on international standards over similar developments and design the steadiest technical architecture for the assignment following the concept of centralized data storage and complete the development with a smooth deployment approach.

4. Scope of Work;

4.1. The consultancy firm shall conduct a detailed study over the existing setup of the current GIC portal and get a clear understanding over the new development requirement at the conceptual, functional as well as the architectural level

4.2. The consultancy firm shall research over the conceptually similar international level developments, study publications over project lessons learnt and incorporate them into the solution definition.

4.3. The conceptual, functional and the architectural level design with the technology stack needs to be discussed with ICTA and shall be added to the solution definition of the proposed development

4.4. The solution definition shall be approved by ICTA in order to proceed for development

4.5. It is expected to incorporate the latest technology as well as communication channels within the proposed GIC portal in a way that it contributes faster information delivery to end user *(Refer Annex 01)*

4.6. Proposing a steady and flexible content model is required by the consultancy firm where the same shall be approved by ICTA

4.7. The total number of organizations of which information that should be included in the solution will be more than 60 apart from the list of services.

4.8. The content arrangement of the proposed GIC portal as well as the mobile application shall follow “intention-based” data presentation approach, where other user stories also shall be treated at different levels.

4.9. The consultancy firm shall suggest a reliable approach for handling of required translations at the project inception stage, as that the approved resolution by ICTA shall be executed parallel to the development of the proposed GIC portal and mobile application.

4.10. The data feeding mechanism which shall be followed by the government organizations into the central content repository shall be treated as crucial segment at a dependency level, where it needs to be a steady and yet a simple approach. Consultancy firm to propose the same.

4.11. The consultancy firm shall provide required formats for content preparation with guidelines, at the government organization level in all 03 languages.

4.12. The proposed GIC portal and the mobile application shall support Unicode standards.

4.13. The consultancy firm is required to adhere to open standards and Service Oriented Architecture (SOA) principles.

4.14. The consultancy firm shall study and get a clear understanding over the applicable Non Functional Requirements for GIC portal as well as mobile application development *[Refer Annex 02]*.

4.15. The consultancy firm is required to adhere to government web standards *[Refer Annex 03]*

4.16. The consultancy firm is required to adhere to e-Government Policy of Sri Lanka *[Refer Annex 04]*.

4.17. The consultancy firm is required to adhere to LIFe standards *[Refer Annex 05]*.

4.18. The consultancy firm is required to maintain project source code in the ICTA source code management system (SCM).

4.19. The consultancy firm shall adopt a proper application release procedure to release the GIC portal and the mobile application

4.20. The development of GIC portal and the mobile application as per the detailed software requirement specification, shall be done in parallel

4.21. The consultancy firm shall submit the project deliverables as specified under the below item '5 – Deliverables and time lines' for both GIC portal and mobile application development

4.22. The consultancy firm shall submit the development proposals along with estimations and schedules separately for GIC portal development and mobile application development assignments. Further the phase wise deliverables will also be traced separately.

4.23. The GIC portal shall be examined through an Information Security audit followed by the successful production deployment of the solution. The Consultancy firm shall incorporate the suggested fixes by the audit and shall obtain the IS audit certificate in order to mark the successful completion of the project

4.24. The consultancy firm is required to implement the GIC portal and mobile application in collaboration with the SQA consultants appointed by ICTA, or review committee and facilitate the 'Software Project Audit Process' specified by ICTA.

4.25. The consultancy firm shall manage the GIC portal and the mobile applications for a period of one year from the date of launch of each (GIC Web Portal / GIC Mobile Application) adhering to a Service Level Agreement

4.26. The consultancy firm is required to conduct proper knowledge transfer at the end of the management period, where the same needs to be sinned-off with the final service management period.

4.27. The consultancy firm is required to have strong prior experience in Microsoft Azure deployment

4.28. The consultancy firm should provide adequate training over the content upload, management and related tasks, to selected ICTA staff and staff members of the government organizations.

4.29. The proposed solution shall include free none proprietary statistics generating tool (for both the GIC portal and mobile application) that would generate below statistics (but not limited to).

- Number of page loads.
- Number of hits received.
- Pages accessed by the user.
- Visitor's location information.

4.30. The consultancy firm should purchase any licenses/publishing materials required to develop or deploy mobile applications on behalf of ICTA. At the end of the assignment all licenses/publishing materials with the source code should be transferred to ICTA

4.31. All consultants attached to the consultancy firm are required to sign a Non-Disclosure Agreement (NDA) where applicable

4.32. The consultancy firm is required to participate for Project Review Committee meeting and Project Implementation Committee (PIC) Meetings as a member

4.33. The consultancy firm is required to work collaboratively with ICTA and government organizations throughout the tenure of the project duration.

5. Final outputs, Reporting Requirements, Time Schedule for Deliverables;

Project duration shall cover a maximum ceiling of 500 Person Days including requirement gathering, designing, developing and deployment of the GIC portal and the GIC mobile application.

5.a) Consultancy firm is required to submit the following list of deliverables for GIC portal development

No	Deliverables	Phase
5.a.1	GIC Portal Implementation Proposal 5.a.1.1 Total Solution Definition (Covering GIC portal and mobile application)	Inception

	5.a.1.2 Detailed Software Requirement Specification 5.a.1.3 Number of person days of the assignment 5.a.1.4 Implementing schedule 5.a.1.5 QA Plan and Test Cases 5.a.1.6 Operational and back office support requirement, Data feeding mechanism and content formats (gov. organization level) 5.a.1.7 Specifications for devices if required (Eg. Mobile devices, Scanners, etc.) 5.a.1.8 Acceptance criteria for Deliverables, UAT 5.a.1.9 Content model	
5.a.2	5.a.2.1 Design document 5.a.2.2 Data migration and integration plan (if applicable)	Elaboration
5.a.3	5.a.3.1 Proper maintenance of source code in SVN	Construction
5.a.4	5.a.4.1 Solutions installation guide 5.a.4.2 User manual 5.a.4.3 Updated Lanka Gate Help Desk templates (Knowledge Tree and T1 Document) 5.a.4.4 QA Status Report 5.a.4.5 Successful UAT acceptance Criteria 5.a.4.5 IS audit report	Transition
5.a.5	5.a.5.1 Monthly GIC Portal Management Report	Management

5.b) Consultancy firm is required to submit the following list of deliverables for GIC mobile application development.

No	**Deliverables**	**Phase**
5.b.1	Mobile Application Implementation Proposal 5.b.1.1 Requirement specification of the mobile application 5.b.1.2 Number of person days of the assignment 5.b.1.3 Mobile application implementing schedule 5.b.1.4 QA Plan and Test Cases 5.b.1.5 Operational and back office support requirement (if the backend application to be developed) 5.b.1.6 Acceptance criteria for Deliverables and UAT 5.b.1.7 Specifications for devices if required (Eg. Mobile devices)	Inception
5.b.2	5.b.2.1 Design document 5.b.2.2 Data migration and integration plan (if applicable)	Elaboration
5.b.3	5.b.3.1 Proper maintenance of source code in SVN	Construction
5.b.4	5.b.4.1 Solutions installation guide 5.b.4.2 User manual 5.b.4.3 Administrator manual 5.b.4.4 Training to selected user groups (if required) 5.b.4.5 Successful UAT acceptance of the Mobile Application and deployment	Transition
5.b.5	5.b.5.1 Monthly Mobile Application Management Report	Management

Refer http://en.wikipedia.org/wiki/IBM_Rational_Unified_Process for more information about RUP (Rational Unified Process) phases.

6. Services and Facilities Provided by ICTA

6.1 Web-based access to the ICTA SCM system
6.2 Access to staging/ production servers
6.3 Required meeting arrangements

7. Review Committees and Review Procedures

All versions of deliverables will be reviewed by the team appointed by ICTA

References:

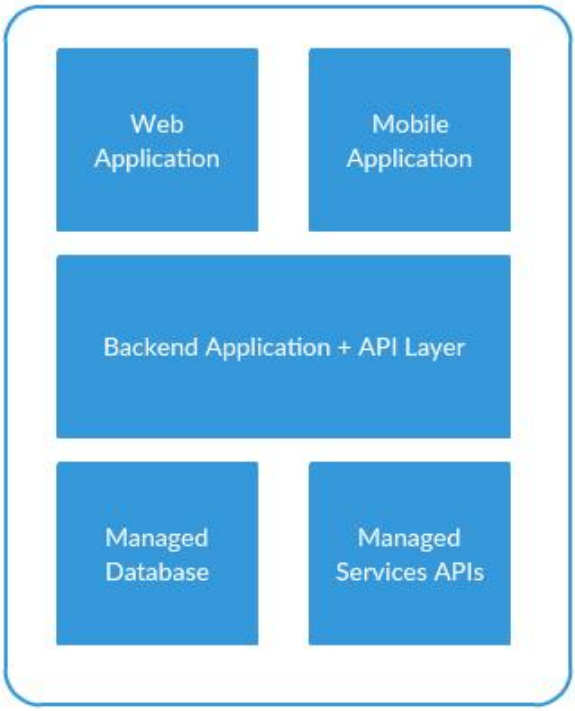
[Annex 1] - Proposed High Level Architecture
[Annex 2] - Non-Functional Requirements
[Annex 3] - Government web standards - https://www.icta.lk/icta-assets/uploads/2016/03/Government_web_standards.v3.pdf
[Annex 4] - eGovernment Policy Approved By Cabinet of Sri Lanka - https://www.icta.lk/icta-assets/uploads/2016/03/eGov-Policy-structured-v4-0.pdf
[Annex 5] - Lanka Interoperability Framework - http://www.life.gov.lk/

– END –

[ANNEX 1]

PROPOSED HIGH-LEVEL ARCHITECTURE

This document describes the proposed high-level technical architecture of the GIC that satisfies technical requirements. Below defines the technologies and techniques necessary to develop and support the system, and to ensure that the system components are compatible and comply with the enterprise-wide standards and direction defined by the ICTA.



Introduction

The above diagram depicts the high-level architecture of the Government Information Center (GIC) and illustrates how the system's components fit into the planned environment.

The Government Information Center (GIC) can be considered as an information repository/platform deployed on cloud where the dissemination of information is done via web and mobile.

The core components and respective technologies of the GIC can be listed as below.

- Web application
- Mobile application
- Backend application with an API layer (REST)
- Database

Core components and technical requirements

- The WordPress can be used as the Content Management System (CMS) which will be deployed in the Azure cloud in a containerized environment to support auto scaling based on the load.

- The citizens who are willing to obtain information will have to interact with the GIC using the web or mobile application.
    - The WordPress frontend should be used with a customized theme as the web application.
    - The mobile application shall be developed using hybrid mobile application development framework such as Ionic or React.

- Backend application should allow the users to manage the content of the GIC. Also, it should consist of an API layer which will be used to communicate with the mobile application and any other external entities.

- Managed Database - Azure Database for MySQL will be used as the data-storage/ database.

- Other technical requirements
    - Any given platform/product which is selected by ICTA should be integrated into the GIC using Representational state transfer (REST) APIs.
    - The custom plugin development should be done to accommodate the requirements that are captured during the requirement study stage.
    - The latest stable versions of the applications/frameworks/products should be used with the approval of ICTA Technical Team.
    - The industry standards and best practices should be followed as and when developing and designing the applications.

- Single-Sign-On (SSO) – This is the platform which will provide the authentication for GIC. It will also be used to provide Single-Sign-On (SSO). These functionalities will be provided as Representational state transfer (REST) APIs in order to be integrated (only to be integrated if required). The platform will be provided by ICTA.

- The above application development should comply with the non-functional requirements stated in the document.

[ANNEX 2]

Non-Functional Requirements

1. SECURITY

1.1. User authentication and authorization

All web applications should be able to access via Lanka Gate and independently via respective department's web site. Any authorization requirement should be implemented within the specific web application.

However the solution should have the provision to integrate with the Lanka Gate Identity Management solution in future.

An administrative application need to be developed wherever applicable.

Wherever applicable internal small applications need to be developed to capture and store relevant data.

1.2. Confidentiality and Integrity

All developed Web applications should ensure "confidentiality" and "integrity" whenever required by adhering to transport and message level security standards. (i.e.: HTTPS, WS-Security)

1.3. Availability

All Web applications should be developed to ensure "High Availability" to remain the system available all the time. (Eg: Web applications clustering capability should be taken into consideration in the development)

1.4. Non-repudiation

All Web applications should ensure non-repudiation by having standard audit-trails and provisions to have WS-Security using digital signatures.

1.5. OWASP Guidelines

All web applications should ensure that the OWASP guidelines for security are followed when designing, developing and deploying the web application.

2. AUDIT FACILITIES

Wherever applicable, an audit trail of all activities must be maintained. On a service or operation being initiated, the system should log the event, creating a basic 'audit log entry'. It should not be possible for the operation to be executed without the log entry being made.

The information recorded in the audit trail depends on the type of activity which takes place. Each service would be responsible for logging detailed information. The different types of operations are -

- Data Capture & Maintenance
- Creation of an entry / item

- Modification an item
- Deletion
- Control (or status change)
- Process execution
- Data synchronization
- Print (only selected item)
- Retrieval
- Monitor

Detail logging may be enabled or disabled for each type of operation, and/or for each business object. It should be possible to configure which attributes of a data item should be traced at the detail level. Tracing of some attributes may be considered mandatory, and they should not be turned off.

3. BACKUP AND CONTINGENCY PLANNING

The main contingencies that should be considered and the training with regards to these shall be given to the relevant staff -

- Equipment failure
- Physical / natural Disaster
- Messaging or communication facilities.
- Changes in operations and policy
- Sudden absence of key personnel
- Breach in Security

Automatic Backups daily, weekly and monthly should be taken. All the backup procedures and backups needs to be tested regularly for restoration.

4. PERFORMANCE

Following performance criteria is provided as a guideline only. If the actual performance is falling below the stipulated figures, the consultant is to justify the reasons. However, the performance level must be accepted by the technical evaluation committee appointed by the client.

The bandwidth is assumed at 512kbps (shared) (point to point between LIX and the Department web service) with 1,000 concurrent users (50% load factor) in total.

Item	Performance
Screen Navigation: field-to-field	< 10 milliseconds
Screen Navigation: screen-to-screen	< 5 seconds
Screen Refresh	< 3 seconds
Screen list box, combo box	< 3 seconds
Screen grid – 25 rows, 10 columns	< 5 seconds
Report preview – (all reports) – initial	< 60 seconds in most instances. It is

page view (if asynchronous)	understood that complicated / large volume reports may require a longer period
Simple enquiry – single table, 5 fields, 3 conditions – without screen rendering	< 5 seconds for 100,000 rows
Complex enquiry – multiple joined table (5), 10 fields, 3 conditions – without screen rendering	< 8 seconds for 100,000 rows
Server side validations / computations	< 10 milliseconds
Client side validations / computations	< 1 millisecond
Batch processing (if any) per 100 records	< 120 seconds
Login, authentication, and verification	< 3 seconds
Daily backups (@ Dept.) – max duration	1 hour (on-line preferred)
Total Restore (@Dept.) – max duration	4 hours

5. USABILITY

The web application should be extremely usable, even a greenhorn user should be able to handle the system and incorporate all the functionality of the system in a simple and user friendly interface. The web application should be internationalized and localized if needed. The web application should be responsive where it should be viewable on any computing device.

6. WEB INTEROPERABILITY

The web application should be able to view in standard compatible web browsers.

7. AVAILABILITY

The web application should be performed as follows,

- 99.99% available unless the web application is designed with expected downtime for activities such as database upgrades and backups.
- Hence to have high availability, the web application must have low downtime and low recovery time.

8. ROBUSTNESS

The web application should be able to handle error conditions gracefully, without failure. This includes a tolerance of invalid data, software defects, and unexpected operating conditions.

9. MAINTAINABILITY

The code of web application should be properly documented with appropriate comments and no complex codes (highly cohesive and loosely coupled) to do modifications such as corrections, improvements or adaption.

10. REUSABILITY

The web application should be able to use of existing assets in some form with the software product development process. Assets are products and by-products of the software development life cycle and include code, software components, test suites, design and documentation.

11. INTERNATIONALIZATION

The web application should be able to access in Sinhalese, English and Tamil. The web application should be able to view in a usable manner in all three languages.

12. API MANAGEMENT

12.1. API Standards and Best Practices

API standards and best practices that *should be adhered* to the code.

12.2. API Security

The web application should be used appropriate API security protocol mentioned below.

- Basic API authentication
    - Basic authentication should never be used without TLS (formally known as SSL) encryption as username and password combination can be easily decoded otherwise.
- OAuth1.0a
    - Uses cryptographic signature value that combines the token secret, nonce, and other request based information. Can be safely used without SSL.
    - Recommend for sensitive data applications
- OAuth2
    - No need to use cryptographic algorithms to create, generate and validate signatures as all the encryption handled by TLS.
    - Recommend for less sensitive data applications
- JWT (JSON Web Tokens)

13. OTHER

W3C standards should be followed where applicable.

BIBLIOGRAPHY

1. The White House. *White House Web API Standards*. Washington, D.C.: github.com, 2015. Print.