Brief Terms of Reference
Conducting Annual Audits for National Certification Authority (NCA) of Sri Lanka
ICTA/GOSL/CON/QCBS/2017/15

1. Introduction

With the rapid adoption of commercial ICT-based services by the local populace and the introduction of e-government in the country, it is expected that electronic commerce will grow substantially in the coming years.

This also raises the probability of identity theft, financial fraud and other security breaches. To counter this, the ICTA in collaboration with Sri Lanka CERT | CC and other stakeholders has initiated a project to establish a national framework which defines legal, administrative and technical regulations for granting, managing and enforcing the use of digital certificates to establish the identities of e-services users with the intention of minimizing electronic fraud.

The electronic transactions act no. 19 of 2006 grants authority for Information and Communication Technology Agency (ICTA) to perform the function of the Root Certification Authority of Sri Lanka called "National Certification Authority (NCA)".

The issuance of digital certificates is to be performed through certified third party certificate service providers (CSPs), who are to be accredited by the NCA.

To enhance the operations of NCA and make sure that certificates issued under NCA are recognized internationally, including web browser vendors (Browser forum), NCA seeking to be WebTrust certified. WebTrust is one of the standards for 'certification authority practice and operations'. Even though there are other standards for the same, NCA prefer to be in line with WebTrust standards, as recommended by the NCA working committee and approved by the Task Force of the NCA project.

2. Objectives

The objectives of this project are to provide consultancy services for auditing and facilitating to obtain WebTrust Seal/Certificate for NCA for a period of three (03) years.

3. Scope of Work

3.1. Perform a preliminary assessment based on the "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0" or the latest version as of the time of the audit. The preliminary audit must be carried out on NCA of Sri Lanka.

Vulnerability assessment and penetration test (VAPT) should also be performed on the NCA systems being audited.

After the preliminary assessment, the consultant must provide recommendations to resolve all issues identified during the preliminary assessment. The assessment must include all topics stated in the above standard.

The consultant must also provide all necessary advisory services which include but not limited to

a) Study the current status of the implementations of NCA and gap analysis against the standards
b) Review architecture, designs and processes
c) Supporting development/verification of policies and required documentation for WebTrust
d) Supervising the NCA implementation to be in compliance with the standards
e) Verification of the deployed solution
f) Assist to resolve the gaps identified during the assessment

Client will implement the recommendations made by the consultant and the consultant shall validate them after conducting a comprehensive audit to enable the issuance of the WebTrust seal.

3.2. The Consultant shall perform subsequent annual independent assessments on NCA based on the "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0" or the latest version as of the time of the assessment. The assessment must include all topics stated in the standard. Vulnerability assessment and penetration test should also be performed on the NCA systems being audited.

The consultant must provide recommendations to resolve all issues identified during the audit. The audit must include all topics stated in the standard. Client will implement the recommendations made by the consultant and the consultant shall validate them to enable the issuance of the WebTrust seal.

3.3. The consultant shall perform all the related activities which WebTrust auditor should contribute and shall facilitate to obtain WebTrust seals from CPA (Chartered Professional Accountant) Canada for the NCA annually for three (03) years.

4. Qualification of the Consulting firm/Lead Auditor

The consulting firm or Lead Partner firm if it is a JV must possess all of the following qualifications.

4.1. The consulting firm is a licensed WebTrust practitioner.

4.2. The consulting firm must be enlisted on the WebTrust website (http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx) or the firm must present a document certifying that it is a certified WebTrust practitioner from CPA Canada.

5. Deliverables

The consulting firm must provide the following outputs.

5.1. Project plan: the plan shows the tasks and time related to the tasks.

5.2. Preliminary assessment report/s: the results of the preliminary assessment of NCA.

5.3. Annual Audit report/s: the results of the independent assessment of NCA.

5.4. VAPT report: the report on the Vulnerability assessment and penetration test performed on the system being assessed. The report must include instructions to address the identified vulnerabilities.

5.5. WebTrust seal: the seal issued by CPA Canada and the publication of the seal on the WebTrust website.

6. Time-line

The selected consultant is required to complete the project with all the deliverables within five (05) months from the contract effective date for the first year and within 2 months for the second year and third year before the expiry of the previous year seal.

No	Deliverable/Activity	Time-Line (year 1)	Time-Line (year 2)	Time-Line (year 2)
1	Kick-off	Complete by [ED+1 week]	-	-
2	Project plan	Complete by [ED+2 weeks]	-	-
3	Preliminary assessment report/s	Complete by [ED+ 8 weeks]	-	-
4	VA report/s	Complete by [ED+ 10weeks]	Complete by [SED-7 weeks]	Complete by [SED-7 weeks]
5	Annual audit report/s	Complete by [ED+ 18 weeks]	Complete by [SED-3 weeks]	Complete by [SED-3 weeks]
6	WebTrust Seal	Complete by [ED+ 20 weeks]	Complete by [SED-1 weeks]	Complete by [SED-1 weeks]

Table 6.1

ED – Contract Effective Date
SED- Seal (WebTrust) Expiry Data

7. Qualifications of the key consultants

Minimum Qualifications for the project team:

Key Professional Staff	**Academic and Professional Qualifications**	**Experience in the PROPOSED ROLE**	**Experience in working in National /Enterprise level projects**
Project Manager	B.Sc or equivalent and CISSP or CISM and ITILv3 or PMP Certification	5 years	3 projects
Certified Security Consultant	B.Sc or equivalent and SANS / (ISC)2 / EC-Council or Other Certified Security Certification	3 years	3 projects
Systems Architect	B.Sc or equivalent and Certification MCSE / RHCE	3 years	2 projects
Senior Network Engineer	B.Sc or equivalent and Vender Certificates related to Networking	3 years	2 projects
Senior Information Security Engineer	B.Sc or equivalent and CISSP/CEH/CCNA/CISM/ MCSE/RHCE Certification	2 years	2 projects

Information Security Auditor	B. Sc or equivalent and CISA	2 years	1 projects
Senior Business Analyst	B. Sc or equivalent	3 years	2 projects
Quality Assurance Manager	B. Sc or equivalent -–	3 years	1 project

8. Services and Facilities Provided by ICTA and Sri Lanka CERT

a) Access to NCA infrastructure and documents will be provided under the strict supervision of Sri Lanka CERT and other relevant parties
b) Desk space with Internet connectivity will be provided at ICTA office.

9. Review Committees and Review Procedures

The consultant is required to work closely with the team at ICTA and Sri Lanka CERT|CC and/or any other review committee(s) as appointed/decided by ICTA/Sri Lanka CERT|CC.

All versions of deliverables will be reviewed and the acceptance will be given once the deliverables meet the acceptance criteria. All activities will also be supervised and signed-off by ICTA and Sri Lanka CERT|CC and/or any other committee(s) as appointed/decided by ICTA/Sri Lanka CERT|CC.