Terms of Reference

Conducting Security Audits for Government Websites: Vulnerability Assessments and Penetration Tests

1. Introduction

Information and Communication Technology Agency of Sri Lanka (ICTA) with the collaboration of the Sri Lanka Computer Emergency Response Team Co-ordination Centre (Sri Lanka CERT||CC), and the Ministry of Telecommunication and Digital Infrastructure (MTDI), aims to implement a project to conduct vulnerability assessments and penetration tests (VAPT) for all government websites in order to identify possible security threats and provide recommendations to address those possible security vulnerabilities. Initially, the assessment will be carried out on all central government Ministries and Departments websites.

The assignment will be carried out in three phases. In the first phase, an initial audit report will be prepared by the firm by assessing the security vulnerabilities of the government websites. In the second phase, government organization will be informed on the security vulnerabilities in their websites and requested to fix those vulnerabilities. Once the security loopholes are fixed by individual organizations, in the third phase follow up audit will be carried out to ensure whether identified security issues have been sufficiently addressed.

For this purpose, ICTA aims to select a firm who has sufficient experience in conducting VAPTs for websites.

2. Aim and Objectives

The primary aim of this assignment is to conduct VAPT to identify any vulnerabilities and weaknesses in the government websites and web applications.

Objectives are,

- to provide initial audit reports to government organizations by assessing current security status of their websites,
- to advice government organizations on fixing the identified security issues (if any), and
- to conduct follow-up audits to examine whether identified security issues have been sufficiently addressed and issue a certificate.

3. Scope of the Work

Phase One:

- Conduct initial VAPTs for assigned websites and produce reports on the security issues exist in the websites and provide recommendations on how to fix those issues.

Phase Two:

- As per the recommendations given by the consultancy firm, government organizations will fix identified security issues.

Phase Three

- Conduct follow-up VAPTs for the government organizations who have fixed those security issues and provide reports. The organizations who have successfully fixed the security issues shall be issued a certificate.

4. Activities to be Carried Out

a. The consultant should conduct the assessment by following industry standards and as per the open web application security project (OWASP) methodology. For this purpose, consultant shall,
   i. use a combination of automated and manual tests
   ii. assessments should be carried out with White, Grey and Black-box approaches when applicable
   iii. identify the security vulnerabilities which may be discovered in the website and web applications including but not limited to Cross-site scripting, Broken ACLs/Weak session management, Buffer Overflows, Forceful browsing, CGI-BIN manipulation, Form /hidden field manipulation, Command injection, Insecure use of cryptography, Cookie posing, SQL injection, Server miss-configuration, Well-known platform vulnerabilities, Errors triggering sensitive information leak etc.

b. The consultant should exploit above vulnerabilities as proof of concept without disturbing the operations.

c. The consultant should identify and prioritize various risks to the given web sites

d. The consultant should identify remedial solutions and provide recommendations to make the web sites secure

e. The consultant should support the respective web site developers to fix/rectify the identified issues thereby enhancing the overall security

f. The consultant is required to reassess the web sites after implementing the recommendations (Phase three as noted above)

g. The consultant is required to sign a non-disclosure agreement with ICTA and respective government organizations.

5. Approach, Timeline, Deliverables and Payment Schedule

5.1. Approach

VAPT will be carried out in three (3) phases.

Phase One: Initial VAPT is to identify any security issues and provide recommendations for government organizations to fix any security issues.

- Consultant is required to complete approximately 120 VAPTs for government websites within 12 weeks.
- The consultant is required to propose two (2) key teams with support staff as per the time schedule given. Each team is required to undertake 60 sites to work in parallel as shown in the Work Schedule (Table 1 Work schedule).
- Each team should complete initial VAPTs in batches (a batch contains 20 websites).
- Upon the completion of the Initial VAPTs for 20 sites (a batch), payment will be released based on the acceptance of the deliverable.
- The consultant is required to propose total cost per website for Initial VAPT.

Phase Two: Upon the completion of the Initial VAPTs for each batch, the government organizations will be advised to fix security issues raised by the consultant within 24 weeks.

Phase Three: The consultant is required to conduct follow-up VAPTs to examine whether government organizations have fixed identified errors in the Initial VAPT and provide a certificate on the current security status of the website.

- Number of VAPT audits would be depending on the response of the government organizations.

- For conducting follow-up VAPTs, the consultant is required to deploy the same key teams (2 teams) undertook the initial VAPTs.

- Upon the completion of the Follow-up VAPTs of batches (20 sites), payments will be released based on the acceptance of the deliverable.

- The consultant is required to complete the Follow-up audits in 8 weeks.

- The consultant is required to propose <u>total cost per website for Follow up VAPT</u>.

Table 1. Work Schedule

<table>
<tr><td colspan="4">←---------- 44 weeks ----------→</td></tr>
<tr><td colspan="3"><u>Initial VAPT</u>

Consultancy Team 1: 60 sites</td><td rowspan="2"></td><td><u>Follow-up VAPT</u>

Consultancy Team 1</td></tr>
<tr><td>Weeks 4</td><td>Weeks 4</td><td>Weeks 4</td><td>Complete all assigned sites in 8 weeks and issue certificates</td></tr>
<tr><td>1 batch (i) (20 Sites)</td><td>1 batch (ii) (20 sites)</td><td>1 batch (iii) (20 Sites)</td><td rowspan="4">Upon the completion of VAPTs for each batch, the government organizations will be given 24 weeks to fix errors.</td><td></td></tr>
<tr><td colspan="3">Consultancy Team 2: 60 sites</td><td>Consultancy Team 2</td></tr>
<tr><td>Weeks 4</td><td>Weeks 4</td><td>Weeks 4</td><td>Complete all assigned sites in 8 weeks and issue the certificates</td></tr>
<tr><td>1 batch (iv) (20 Sites)</td><td>1 batch (v) (20 Sites)</td><td>1 batch (vi) (20 Sites)</td><td></td></tr>
</table>

5.2. Timeline and Payment Schedule

Consultant will be engaged for a period of **44 weeks**.

#	Activity	Deliverable	Timeline	Payment Schedule
Phase One – Initial VAPT				
1	Conduct Initial VAPT for all websites	- VAPT Report for individual organization with recommendations	12 weeks for all sites	100% of the cost of Initial VAPT

		(Note 1)		
Phase Two: Government organizations fix security issues in government websites				
Phase Three – Follow-up VAPT				
2	Conduct Follow up VAPT websites (Phase Two as noted in the section 3: Scope of Work)	- Security Certificate - Reassessment VAPT Report for individual organization with recommendations (Note 1)	8 weeks for all sites	100% of the cost of Follow up VAPT

**** Penalties will be enforced for delayed deliverables.

5.3. Deliverable: Structure of the VAPT Report

Note 1:

Structure of the Initial VAPT report/Follow up VAPT report for an individual organization shall contain the following *The consultant however may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process. Reports shall be submitted for individual site.*

i. *Identification of Auditee (Address & contact information) and respective web site*
ii. *Personnel involved in the audit*
iii. *Dates and Locations of VAPT*
iv. *Terms of reference*
v. *Standards followed*
vi. *Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, penetration testing, application security assessment, website assessment, etc.)*
    - *Tools used and methodology employed*
    - *Positive security aspects identified*
    - *List of vulnerabilities identified*
    - *Description of vulnerability*
    - *Risk rating or severity of vulnerability*
    - *Category of Risk: Very High / High / Medium / Low*
    - *Test cases used for assessing the vulnerabilities*
    - *Illustration of the test cases*
    - *Steps followed for exploiting the above vulnerabilities*
    - *Applicable screenshots/evidences/ documents etc.*
vii. *Recommendations for corrective action*

**** Vendors are required to address each of the above criteria in the evaluation report (VAPT).

6. Qualification of the Key Consultants

Minimum qualification and experience of the staff is tabulated below. Consultant, however, propose any number of staff to complete the deliverables as stated in the Terms of Reference (TOR).

#	Consultants	Minimum Number of Staff	Minimum Qualification	Experience
1	Project Manager [For Phase 1 & 2]	1	Graduate in Engineering/IT/IS or related discipline. Project Management Professional (PMP) / ITILv3 certification would be an advantage.	Minimum 5 years of experience in managing IT projects, And demonstrated 3 years of experience in managing Security Audits.
Phase 1: Initial VAPT				
2	Senior Security Engineer	2 [Team 1 and Team 2]	B.Sc in IT/IS, Engineering or related degree, And, more than one certificate on the following: Certified Information System Auditor (CISA),	Demonstrated more than 5 years of experience in security audits

			Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Computer Forensic Examiner (CCFE)	
3	Security Auditor/Engineer/ Analyst	6 For Two teams (Minimum 3 Members per team)	BSc degree in IT/IS or relevant field, And at least one certification on the following: CISA, CISSP, CEH, or CCFE	3 years of experience in the information systems security audits.
Phase 3: Follow-up VAPT				
4	Senior Security Engineer	2 [1 consultant per team]	Same as above	Same as above
5	Security Auditor/Engineer/ Analyst	6 For Two teams (Minimum 3 Members per team)	BSc degree in IT/IS or relevant field, And at least one certification on the following: CISA, CISSP, CEH, or CCFE	3 years of experience in the information systems security audits.

7. Inputs from ICTA

a. ICTA shall provide a list of URLs.

b. ICTA and respective government organizations will provide authorization to conduct website audits.

8. Review Process

- Deliverables will be reviewed by a team jointly appointed by the ICTA and Sri Lanka CERT (C|C).

9. Number of Websites

Number of websites would be 120 (Number of websites would slightly change).