## 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 Coordination 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
  - 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 <u>non-disclosure agreement</u> 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.

**<u>Phase One:</u>** 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.
- $\circ$  The consultant is required to propose <u>total cost per website for Initial</u> <u>VAPT</u>.

**<u>Phase Two:</u>** 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.

**<u>Phase Three:</u>** 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.
- $\circ$ 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</u> <u>up VAPT</u>.

← 44 weeks →				
Initial VA	<u>PT</u>			Follow-up VAPT
Consultancy Team 1: 60 sites				Consultancy Team 1
Weeks 4	Weeks 4	Weeks 4	24 weeks	Complete all assigned sites
1 batch	1 batch	1 batch	Upon the completion	in 8 weeks and issue
<i>(i)</i>	( <i>ii</i> )	( <i>iii</i> )	of VAPTs for each	certificates
(20	(20	(20	batch, the government	
Sites)	sites)	Sites)	organizations will be	
Consultancy Team 2: 60 sites			given 24 weeks to fix errors.	Consultancy Team 2
Weeks 4	Weeks 4	Weeks 4		Complete all assigned sites
1 batch	1 batch	1 batch		in 8 weeks and issue the
(iv)	(v)	(vi)		certificates
(20	(20	(20		
Sites)	Sites)	Sites)		

Table 1. Work Schedule

## 5.2. Timeline and Payment Schedule

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

#	Activity	Deliverable	Timeline	Payment Schedule
Phi	ase 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

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

Image: second				Certified	
Image: Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Computer Forensic Examiner (CCFF)Image: Security Forensic Examiner (CCFF)3Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And information experience in the and 3 Members per team)3 years of experience in the audits. CISSP, CEH, or CCFE4Senior Security Engineer2 [1 consultant per team]Same as aboveSame as above experience in the information5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or ISSP, CEH, or CCFESame as above4Senior Security Auditor/Engineer2 (11 consultant per team]Same as aboveSame as above experience in the information5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, AndSame as above5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS critication on the audits.					
4   Security   6 For Two   BSc degree in IT/IS   3 years of     3   Security   6 For Two   BSc degree in IT/IS   3 years of     Analyst   6 For Two   BSc degree in IT/IS   3 years of     Multor/Engineer/   teams   or relevant field,   experience in the     Analyst   Minimum   at least one   systems security     3 Members   certification on the   audits.     per team)   following: CISA,   CISSP, CEH, or     CISP, CEH   Or relevant field,   Same as above     Engineer   [1   consultant     per team]   Same as above   Same as above     5   Security   6 For Two   BSc degree in IT/IS   3 years of     4   Senior Security   2   Same as above   Same as above     5   Security   6 For Two   BSc degree in ITI/IS   3 years of     4   Security   6 For Two   BSc degree in ITI/IS   3 years of     5   Security   6 For Two   BSc degree in ITI/IS   3 years of     4   Security   6 For Two   BSc degree in ITI/IS				5	
Image: Security6 For Two (CEH), Certified Computer Forensic Examiner (CCFE)3 years of experience in the information3Security6 For Two teamsBSc degree in IT/IS or relevant field, Analyst3 years of experience in the information3Memberscertification on the per team)systems security audits.4SeniorSecurity Parier2 [1 consultant per team]Same as above5Security Auditor/Engineer/6 For Two a get and the systemsSame as above audits.6SeniorSecurity audits.2 audits.Same as above7SeniorSecurity auditor/Engineer/2 auditor/Engineer/Same as above audits.5Security Auditor/Engineer/6 For Two teamsBSc degree in IT/IS auditor/Engineer/3 years of audits.5Security Auditor/Engineer/6 For Two teamsBSc degree in IT/IS a years of audits.3 years of audits.5Members Auditor/Engineer/6 For Two teamsBSc degree in IT/IS a years of audits.3 years of audits.				5	
Image: second				<b>`</b>	
Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information(Minimum 3 Membersat least one per team)systems security audits.4Senior Security2 11 consultant per team]Same as above or relevant field, audits.5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And9Senior certification on the per team]Same as above certification9Senior Forgineer2 [1] consultant per team]5Security Auditor/Engineer/ Analyst6 For Two teamsSc degree in IT/IS or relevant field, And5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information6For Two Auditor/Engineer/ Analyst10 certification on the per team)3 years certification on the audits.					
Image: second				· · · ·	
1   Image: Complexity of the second of the				_	
3   Security   6 For Two   BSc degree in IT/IS   3 years of experience in the information     3   Auditor/Engineer/   teams   or relevant field, And   information     Analyst   (Minimum   at least one systems security audits.   systems security audits.     3   Members   certification on the following: CISA, CISSP, CEH, or CCFE   audits.     Phase 3: Follow-up VAPT   2   Same as above   Same as above     4   Senior Security 2   Same as above   Same as above     5   Security   6 For Two   BSc degree in IT/IS   3 years of experience in the information     5   Security   Analyst   CISSP, CEH, or CEIA, or CCFE   Same as above     5   Security   6 For Two   Same as above   Same as above     5   Security   6 For Two   BSc degree in IT/IS   years of experience in the information     Analyst   Itams   or relevant field,   experience in the information     4   Mitor/Engineer/   Teams   or relevant field,   experience in the information     5   Security   6 For Two   BSc degree in IT/IS   years of experience in the information <th></th> <td></td> <td></td> <td></td> <td></td>					
Auditor/Engineer/   teams   or relevant field,   experience in the information     Analyst   (Minimum   at least one   systems security     3 Members   certification on the following: CISA,   audits.     following: CISA,   CISSP, CEH, or   information     certification   or relevant field,   audits.     following: CISA,   CISSP, CEH, or   information     certification   or relevant field,   audits.     following: CISA,   CISSP, CEH, or   information     following: Security   2   Same as above   Same as above     following: CISA,   [1]   consultant   information     per team]   per team]   Same as above   Same as above     5   Security   6 For Two   BSc degree in IT/IS   3 years of     Anditor/Engineer/   iteams   or relevant field,   experience in the     Analyst   And   information   information     Analyst   And   information   information     And   information   information   information     Anditor/Engineer/   Amd   certification on					
AnalystAndinformationAnalyst(Minimum 3 Members per team)at least one following: CISA, CISSP, CEH, or CCFEaudits.Phase 3: Follow-up VAPT2 [1] consultantSame as aboveSame as above4Senior per team)2 per team]Same as aboveSame as above5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information6(Minimum Andat least one informationsystems security audits.3Members per team)CISSP, CEH, or1	3	2	6 For Two		5
Y(Minimum at at berteam)at centification on the following: CISA, CISSP, CEH, or CCFEsystems security audits.4Senior Security2Same as aboveSame as above4Senior Security2Same as aboveSame as above4Senior Security1II4Senior Security2Same as aboveSame as above5Security6For TwoBSc degree in IT/IS3 years of or relevant field,5Security6For TwoBSc degree in IT/IS3 years of or relevant field,6Muditor/Engineer/ (MinimumAndinformation7AnalystIAndinformation8Gerteam)Gillowing: CISA, per team)Gillowing: CISA, CISSP, CEH, orinformation		0	teams		-
A Members per team)certification on the following: CISA, CISSP, CEH, or CCFEaudits.4Senior Security Engineer2Same as aboveSame as above5Security ner team]6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information5Security Auditor/Engineer/ Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information5Security Analyst6 For Two teamsBSc degree in IT/IS or relevant field, And3 years of experience in the information6For Two teamsBSc degree in IT/IS or relevant field, AndSystems security audits.		Analyst		And	information
Image: series of the series			(Minimum	at least one	systems security
Image: A series of the serie			3 Members	certification on the	audits.
i   i   cCFE   i     i   Senior Security   i   Same as above   Same as above     i   Senior Security   i   Same as above   Same as above     i   Senior Security   i   Same as above   Same as above     i   Senior Security   i   I   I   I     i   Engineer   I   I   I   I   I     i   I			per team)	following: CISA,	
Image: A series of the serie				CISSP, CEH, or	
4   Senior   Security   2   Same as above   Same as above     4   Senior   Security   [1   Image: Consultant information   Image: Consultant information     5   Security   6 For Two   BSc degree in IT/IS   3 years of experience in the information     5   Security   6 For Two   BSc degree in IT/IS   3 years of experience in the information     6   Auditor/Engineer/   teams   or relevant field,   experience in the information     7   Analyst   Image: Cisse in IT/IS   systems security     8   Image: Cisse in IT/IS   systems security     9   Image: Cisse in IT/IS   systems security     9   Image: Cisse in IT/IS   systems security     9   Image: Cisse in IT/IS   sudits.				CCFE	
Engineer[1	Pha	ase 3: Follow-up VAP	ſ		
Image: second	4	Senior Security	2	Same as above	Same as above
Image: securityper team]Image: securitySecurity6 For TwoBSc degree in T/IS3 years ofAuditor/Engineer/teamsor relevant field,experience in theAnalystImage: securityAndinformationImage: security3 Memberscertification on theaudits.Image: securityper team)following: CISA,Image: securityImage: securityImage: securityCISSP, CEH, orImage: security		Engineer	[1		
5Security6 For TwoBSc degree in IT/IS3 yearsofAuditor/Engineer/teamsor relevant field,experience in theAnalystAndinformation(Minimumatleastone3 Memberscertification on theaudits.per team)following: CISA,CISSP, CEH, or			consultant		
Auditor/Engineer/teamsor relevant field,experience in theAnalystAndinformation(Minimumatleastone3 Memberscertification on theaudits.per team)following: CISA,CISSP, CEH, or			per team]		
AnalystAndinformation(Minimumat least onesystems security3 Memberscertification on theaudits.per team)following: CISA,CISSP, CEH, or	5	Security	6 For Two	BSc degree in IT/IS	3 years of
(Minimumatleastonesystemssecurity3 Memberscertificationontheaudits.per team)following: CISA,CISSP, CEH, orcertification		Auditor/Engineer/	teams	or relevant field,	experience in the
3 Members certification on the audits. per team) following: CISA, CISSP, CEH, or		Analyst		And	information
per team) following: CISA, CISSP, CEH, or			(Minimum	at least one	systems security
CISSP, CEH, or			3 Members	certification on the	audits.
			per team)	following: CISA,	
				CISSP, CEH, or	
				CCFE	

# 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).