The purpose of this invitation to quote (ITQ) is to invite experienced vendors to submit their quotation for ISCA Vulnerability Assessment and Penetration Testing (VAPT).

## 1. Scope of work

ISCA would like to engage external expertise to conduct a Vulnerability Assessment and Penetration Testing for ISCA Information Technology assess.

1. Network vulnerability assessment/ Penetration testing
2. Web application penetration test

The detail requirements are in below:

### 1.1 ISCA Network vulnerability assessment

ISCA would like to conduct a vulnerability assessment for ISCA's IT network assess the network against authorize access and malware attack. The scope of the IT network will cover:

1. Network segment for ISCA staff both through LAN and Wireless
2. Network segment for ISCA member access internet through ISCA computer
3. Internet access by ISCA member through ISCA member network
4. ***16 physical / virtual machines servers***

The Testing shall minimally include the following areas of vulnerabilities:

a. Leakage of Confidential information
b. Violation of systems/applications access rights
c. Compromise of Integrity of the systems/applications and information
d. Malicious content infiltration
e. Network access control subversion
f. Denial of Service (DoS) (Layer 3,4 and 7)
g. Subversion of host and network intrusion detection/prevention systems
h. Insecure authentication and session management
i. Insecure cryptographic storage
j. Security misconfiguration (include insufficiently harden)

### 1.2 ISCA Web application penetration test

**Conduct 4 web applications penetration testing that includes *ISCA corporate website & Membership Portal (Salesforce)***. The scope of the web application penetration testing shall include the following areas of vulnerabilities:

a. Buffer overflows;
b. Denial of Service (DoS);

c. Insecure access control mechanism (e.g. account privilege escalation, failure to restrict URL access and etc);
d. Malicious code injection (e.g. SQL injection, Cross-Site Scripting and etc);
e. Cross-Site Request Forgery (CSRF);
f. Cross-Frame Scripting (CFS);
g. Insecure authentication and session management;
h. Insecure direct object references;
i. Insecure cryptographic storage;
j. Insufficient transport layer protection (e.g. enabling of weak cipher suite in the SSL protocol);
k. Invalidated redirects and forwards;
l. Improper error and exception handling;
m. Security misconfiguration
n. application logic flaws.

The Tenderer shall also take the latest Open Web Security Application Project (OWASP) Application Verification security requirement into consideration when determining the areas of vulnerabilities to be tested.

## 2. Required Information

Please provide following info in the quotation:

- Approach and Methodology
- Vulnerability Assessment and Penetration Test Tools
- Project schedule

## 3. Deliverables

a. VAPT reports.
b. Detailed results for vulnerabilities discovered, exploited vulnerabilities and proof of concepts/screenshots.
c. Detailed explanations of the implications of findings, business impacts and risks for each of the identified exposures.
d. Remediation recommendations to the gaps identified.
e. Detailed steps (wherever applicable) to be followed when mitigating the reported issues.

## 4. Quotation Validity

Quotations submitted must be valid for 3 months from the date of opening of ITQ**.**

## 5. Disclaimers

ISCA shall be under no obligation to accept the quotation with the lowest quote or enter into correspondence with any vendor regarding the reason for non-acceptance of quotation.

ISCA reserves the right, unless the vendor expressly stipulates to the contrary in its quotation, to accept only such portion(s) of a quotation as ISCA may in its sole discretion decide and the quotation shall be adjusted accordingly.

## 6. Enquiries

For any enquiry or submission, please email to **ict.tenders@isca.org.sg** with the subject "***ICT-14-2020***" before the closing date.
Closing date: 09 October 2020, 5pm