INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS
60 Cecil Street, ISCA House
Singapore 049709
Tel: 65 6749 8060
isca.org.sg

ICT-10-2025 ISCA Vulnerability Assessment and Penetration Testing (VAPT)

The purpose of this invitation to quote (ITQ) is to invite experienced vendors to submit their quotations for the Institute of Singapore Chartered Accountants, (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 the ISCA Information Technology assessment, preferably lead by a CREST certified professional.

1. Network Vulnerability Assessment and Penetration Testing
2. Web application Vulnerability Assessment

1.1 Network Vulnerability Assessment and Penetration Testing

The details requirements are below:

1. Network segment for ISCA staff both through LAN and Wireless
2. 6 critical physical/virtual machines servers

The Testing shall minimally include the following areas of vulnerabilities:

- Leakage of Confidential information
- Violation of systems/applications access rights
- Compromise of Integrity of the systems/applications and information
- Malicious content infiltration
- Network access control subversion
- Denial of Service (DoS) (Layers 3,4 and 7)
- Subversion of host and network intrusion detection/prevention systems
- Insecure authentication and session management
- Insecure cryptographic storage
- Security misconfiguration (including insufficiently harden)

1.2 Web Application Vulnerability Assessment

Conduct web applications penetration testing which includes ISCA corporate website. The scope of the web application penetration testing shall include the following areas of vulnerabilities:

- Buffer overflows
- Denial of Service (DoS)
- Insecure access control mechanism (e.g., account privilege escalation, failure to restrict URL access and etc)
- Malicious code injection (e.g., SQL injection, Cross-Site Scripting and etc)
- Cross-Site Request Forgery (CSRF)
- Cross-Frame Scripting (CFS)
- Insecure authentication and session management

- Insecure direct object references
- Insecure cryptographic storage
- Insufficient transport layer protection (e.g., enabling of weak cipher suite in the SSL protocol)
- Invalidated redirects and forwarding
- Improper error and exception handling
- Security misconfiguration
- 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.

Personnel involved in the VAPT are preferably led or have at least a person with CREST certification.

2. Proposal Additional Requirements

Please provide the following information in the proposal quotation:

- Approach and Methodology
- List of the Vulnerability Assessment and Penetration Test Tools use
- Project schedule

3. Deliverables

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

4. Quotations 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 correspondence with any vendor regarding the reason for non-acceptance of the 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.

ISCA reserves the right to make amend, alter, change or repel any of scope of work in this document.

6. Enquiries

For further enquiries and submissions, please email to ict.tenders@isca.org.sg with the subject "ICT-10-2025" before the closing date.

Closing date: 13 March 2025, 12pm