

WEBSITE ASSESSMENT SERVICES FOR SINGAPORE ART
MUSEUM

SAM/ITT/2026/0004

SECTION B: REQUIREMENTS SPECIFICATION

1. PURPOSE

- 1.1. The purpose of this ITT is to procure Website Assessment Services for SAM Websites.

2. DEFINITION OF TERMS

- 2.1. Unless otherwise stated, all requirements shall be treated as mandatory.
- 2.2. Clauses denoted by the word “shall” indicate compulsory requirements to be delivered by the Contractor. Any proposed workaround or alternative solution shall be clearly stated in the Vendor’s tender submission and shall be subject to SAM’s review and acceptance.
- 2.3. The word “**SAM**” refers to Singapore Art Museum.
- 2.4. The word “**Vendor**” or “**Vendors**” refers to companies participating in this ITT.
- 2.5. The word “**Contractor**” refers to the successful Vendor awarded under this ITT.
- 2.6. The words “**SAM Websites**” refers to all websites and microsites operated by Singapore Art Museum.
- 2.7. The acronym “**SOR**” means Schedule of Rates.
- 2.8. The acronym “**ITT**” means Invitation to Tender.
- 2.9. The word “**Tenderer**” refers to a Vendor submitting a tender in response to this ITT.
- 2.10. The words “**Condition of Contract**” refer to Tender Document Section E.

3. REQUIREMENTS FOR CONTRACTOR

- 3.1. **SAM intends to procure Web Application Vulnerability Assessment and Penetration Testing services for its websites (“SAM Websites”), and tenderers shall submit their quotations accordingly.**

- 3.1.1. Tenderers shall provide rates for **Web Application Vulnerability Assessment and Penetration Testing (“VAPT”)** in the form of a **Schedule of Rates (“SOR”)**.
- 3.1.2. The rates quoted for VAPT shall be on a per-assessment test basis for each website.

- 3.2. Website assessment services shall apply to all SAM Websites and shall not be limited to the current development version or current hosting infrastructure. The quoted rates shall remain applicable to subsequent changes in deployment architecture, hosting environment, or website implementation, provided that the nature and scope of the assessment remain substantially similar.

3.3. Web Application Vulnerability Assessment & Penetration Testing (VAPT):

- 3.3.1. The Contractor shall perform Web Application Vulnerability Assessment and Penetration Testing (VAPT) for all SAM Websites within the approved scope. The VAPT shall comprise both:
 - 3.3.1.1. **Automated Vulnerability Assessment (VA)** using industry-recognised web application security scanning tools.
 - 3.3.1.2. **Manual Penetration Testing (PT)** conducted by qualified security professionals to validate findings and identify vulnerabilities not detectable by automated tools.

3.3.2. Vulnerability Assessment (VA) Tools Capabilities – The web application security scanning tool(s) used by the Contractor shall, at minimum, support:

- 3.3.2.1. Web protocols used by the web application systems and services, including but not limited to HTTP, SSL/TLS, HTTP Proxies, and SOCKS proxies, where applicable.
- 3.3.2.2. Authentication services or mechanisms used by the web application systems and services, including but not limited to Basic Authentication, Digest Authentication, HTTP Negotiate, HTML Form-based Authentication, Single Sign-On, Two-Factor Authentication, and Client SSL Certificates.
- 3.3.2.3. Session management used by the web application systems and services, including the ability to maintain a valid session with the system throughout the scanning process, where applicable.
- 3.3.2.4. Automatic crawling of the web application system and services until defines criteria are met or all permissible paths and pages have been discovered and assessed.
- 3.3.2.5. Automatic parsing and mapping of application structure, workflows, and functionalities.
- 3.3.2.6. Automated vulnerability testing covering, but not limited to:
 - 3.3.2.6.1. Configurations weakness
 - 3.3.2.6.2. Authentication vulnerabilities
 - 3.3.2.6.3. Authorisation and access control weaknesses
 - 3.3.2.6.4. Client-side vulnerabilities (e.g. XSS, CSRF, etc.)
 - 3.3.2.6.5. Injection and command-based attacks (e.g. SQL Injection, OS Command Injection, File Inclusion, etc.)
 - 3.3.2.6.6. Information disclosure vulnerabilities
- 3.3.2.7. The automated scanning tool shall be a reputed **Dynamic Application Security Testing (DAST)** solution (recognised in industry analyst report, e.g. Gartner Magic Quadrant Leader), with high accuracy, low false positive, and configurable scan policies.
- 3.3.2.8. The scanning tool shall be updated with vulnerability signatures not more than one (1) month old at the time of assessment and shall be able to map findings to **OWASP Top Ten**, where applicable.
- 3.3.2.9. The tool shall generate reports with clear descriptions of identified vulnerabilities, risk ratings, impacted components, and recommended remediation actions.

3.3.3. Penetration Testing (PT) – Methodology and Scope

- 3.3.3.1. Penetration Testing shall be conducted using **industry-recognised methodologies**, such as but not limited to OWASP, PTES, CREST, etc., and shall emphasise **manual testing and validation** beyond automated scanning results.
- 3.3.3.2. The PT shall be conducted using a **black-box testing approach**, simulating real-world attack scenarios from an external threat actor's perspective, without access to the application source code or internal architecture.
 - 3.3.3.2.1. Manual testing shall include, but not be limited to:
 - 3.3.3.2.1.1. Validation of vulnerabilities identified by automated tools
 - 3.3.3.2.1.2. Identification of business logic flaws not detectable by signature-based scanning
 - 3.3.3.2.1.3. Discovery of chained or context-based attacks
 - 3.3.3.2.1.4. Identification and elimination of false positives
 - 3.3.3.2.1.5. Detection of security weaknesses not covered by automated tools
- 3.3.3.3. The Contractor shall demonstrate adequate understanding of the web application's functionality, workflows, roles, and access paths to ensure effective and meaningful penetration testing.

3.3.3.4. Exploitation activities shall be controlled, non-destructive, and limited strictly to what is necessary to demonstrate impact, without disrupting production services or compromising data.

3.3.3.5. The website vulnerability assessment shall be conducted in Singapore via a valid static source IP address. The results and reports shall reside within Singapore.

3.3.4. General VAPT Requirements

3.3.4.1. All testing activities shall be performed within the approved scope defined by SAM and shall not extend beyond authorised systems, URLs, or environments.

3.3.4.2. The VAPT shall be conducted from **Singapore**, using a **valid static source IP address**.

3.3.4.3. All scan outputs, test results, and reports shall be encrypted, stored and hosted within Singapore.

3.3.4.4. The Contractor shall submit a comprehensive VAPT report covering:

- 3.3.4.4.1. Scope and methodology
- 3.3.4.4.2. Tools and techniques used
- 3.3.4.4.3. Validated vulnerabilities with severity ratings
- 3.3.4.4.4. Evidence and reproduction steps
- 3.3.4.4.5. Recommended remediation measures

3.4. Other Requirements:

3.4.1. SAM conducts VAPT throughout the year (with typical Fiscal Year period of April to March) on a regular basis. The Contractor may expect VAPT requests for SAM Websites during the following periods:

- 3.4.1.1. April to June
- 3.4.1.2. July to September
- 3.4.1.3. October to December
- 3.4.1.4. January to March

3.4.2. SAM shall be entitled to request VAPT for any of SAM Websites at any time during the contract period.

3.4.3. SAM shall be able to request for the performance of VAPT on SAM Websites at the quoted rates (Schedule of Rates) by the vendor.

3.4.4. The following are the current websites and microsites operated by SAM:

- 3.4.4.1. singaporeartmuseum.sg
- 3.4.4.2. singaporebiennale.sg
- 3.4.4.3. theeverydaymuseum.sg
- 3.4.4.4. samplings.sg
- 3.4.4.5. opensystems.sg
- 3.4.4.6. spiralscape.quest
- 3.4.4.7. altpower.sg
- 3.4.4.8. design.singaporeartmuseum.sg
- 3.4.4.9. talkingobjects.singaporeartmuseum.sg

3.4.5. During the contract period, SAM may replace any of the listed websites or microsites with new websites.

- 3.4.6. The Contractor shall commence the VAPT within three (3) working days from SAM's request, and the report shall be provided within five (5) working days from the commencement of the VAPT. Where vulnerabilities are identified, the Contractor shall perform re-scans of the affected website(s) for verification of remediation, for up to five (5) rounds. Any request for extension of time for report submission shall be made by the Contractor in writing and shall be subject to SAM's approval.
- 3.4.7. VAPT services shall only be chargeable where SAM has requested the Contractor to perform the services.
- 3.4.8. The solution shall be standalone and shall not require the installation of any software or hardware on SAM's devices or premises.
- 3.4.9. The solution shall be capable of performing the required assessments from a remote site.
- 3.4.10. The Contractor shall, at its own cost, ensure that its solution used to access or contact the SAM Websites is secure, free from viruses, malware, spyware, and other malicious code, and shall not introduce any security vulnerability, malicious payload, or unauthorised activity to SAM Websites or environment.
- 3.4.11. Under the Singapore Cybersecurity Act 2018, the Contractor shall hold and maintain a valid license issued by the Cybersecurity Services Regulation Office (CSRO), throughout the contract period, for the provision of Penetration Testing Services.
- 3.4.12. The Contractor shall, upon SAM's request, provide documentary proof of such licence, and shall immediately notify SAM in writing if such licence is suspended, revoked, expires, or otherwise ceases to be valid.
- 3.4.13. Contractor shall not subcontract any penetration testing services under this contract without SAM's prior written approval. Any approved subcontractor performing such services shall also hold the required valid licence issued by CSRO for providing Penetration Testing Services.
- 3.4.14. Pen Testers assigned by the Contractor to perform the VAPT services under this Contract shall hold valid CREST certification and relevant industry-recognised penetration testing certifications, such as Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), or Offensive Security Certified Expert (OSCE), or their equivalent.
- 3.4.15. By submitting a proposal for this ITT, Vendors shall be deemed to have understood and complied with all **Requirement Specifications** of this ITT, including the **Conditions of Contract**. Any non-compliance, exception, or deviation shall be clearly and expressly stated in the **mandatory Compliance Checklist** (for Requirements Specifications and Conditions of Contract), which shall form part of the tender submission.
- 3.4.16. Vendors shall submit a sample VAPT report as part of their tender submission. Sensitive Information may be masked.

4. DELIVERABLES

- 4.1 The Contractor shall provide a technical report for each VAPT performed.

5. SERVICE ESCALATION

- 5.1 The Contractor shall provide a service escalation list of personnel's contacts in the event of emergency and/or unsatisfactory service rendered.

6. DELIVERY SCHEDULE

- 6.1 The Contractor shall start delivery of the service within one (1) week of receipt of the Letter of Acceptance/Purchase Order.

7. FEES, PRICE AND PAYMENT SCHEDULE

- 7.1 Fees shall be quoted according to the Payment schedule as indicated in (ANNEX A – PAYMENT SCHEDULE).
- 7.2 Vendors must indicate their proposal fee structure / price as required by this ITT.
- 7.3 Vendors must satisfy themselves before submitting any Proposal Offer as to the correctness and sufficiency of their Offer Price for the execution and complete provision of all goods and/or services required under this ITT.
- 7.4 The Offer Price set out in the Proposal Offer shall be deemed to have included the delivery of all goods and/or the performance of all services to meet the Requirements Specification and Conditions of Contract in full.
- 7.5 Please indicate in your Proposal if you are / are not a taxable person / organisation under the Goods and Services Act and provide your GST registration number.
- 7.6 All Offer Price set out in the Proposal Offer shall have a minimum validity period of 3 months, starting from the Closing Date of this ITT.
- 7.7 Payment shall be made at the end of the month for invoices received by SAM by the 1st of the month. If invoices are received after the 1st of the month, payment shall be made at the end of the following month.

8. ENQUIRIES OR CLARIFICATIONS

8.1. The Representative(s) for this Contract and the corresponding contact details are as follows:

Name, Designation: Mr. Imran, Manager, Information Technology

Email Address: SAM-IT-TenderRFP@singaporeartmuseum.sg

8.2. The Contract may be extended for one or more periods at SAM's sole discretion.

8.3. All official clarifications, enquiries, including replies, shall be made in writing only.

8.4. The Vendor must have a Project Office for the purposes set out in Clause 22 of the Conditions of Contract. The address of the proposed Project Office that will be used for purposes of the Contract must be provided in the ITT Offer.

ANNEX A – PAYMENT SCHEDULE

1) Schedule of Rates (SOR)

Services	Quantity (per VAPT)	Year 1 Pricing (April 2026 to March 2027)	Year 2 Pricing (April 2027 to March 2028)	Year 3 Pricing April 2028 to March 2029
a) Web Application Vulnerability Assessment & Penetration Testing (VAPT) for <u>SAM Websites</u>	1			

Note 1: Invoice to be processed after services rendered.

Note 2: Payment shall be made at the end of the month for invoices received by SAM by the 1st of the month. If invoices are received after the 1st of the month, payment shall be made at the end of the following month.