

REQUEST FOR PROPOSAL

SARS RFP 17-2022

APPOINTMENT OF SECURITY ASSESSMENT SERVICES PANEL

BUSINESS REQUIREMENTS SPECIFICATION

Table of Contents

1	Background	3
2	BUSINESS REQUIREMENT Summary	3
3	Components of Scope.....	3
4	Underlying Principles towards RFP	5
5	Security Process	6

RFP 17/2022

Business Requirements Specification

1 BACKGROUND

In pursuit of our vision to build a smart modern SARS with unquestionable integrity that is trusted and admired, SARS set nine core objectives in support of its mission. These objectives include making it easy for taxpayers and traders to comply with their obligations and the modernisation of SARS systems to provide digital and streamlined online services. A solid security foundation is critical in enabling the organisation to achieve the mission and objectives.

In this RFP, SARS is looking at establishing a panel of Service Providers on a non-exclusive basis to offer Security Assessment Services on software and online applications and services developed by SARS, its designated development partners or other online partners. Successful Bidders will be requested to provide services contained in this RFP as needed by SARS on different projects on an ad-hoc basis.

2 BUSINESS REQUIREMENT SUMMARY

SARS requires the services of competent and capable Service Providers who will complement the work of our Software Quality Management and Testing team in executing the security testing of applications and systems identified by SARS, ensuring security is built in within the Software Development Life Cycle. For the purposes of this RFP, a *security vulnerability is defined as an unintended characteristic of a computing component or system configuration that multiplies the risk of an adverse event or a loss occurring either due to accidental exposure, deliberate attack, or conflict with new system components*. Eradicating software vulnerabilities before a product's release is crucial to SARS. SARS' approach is to build security in from the outset and in the final phase bring in a independent security team for an independent assessment prior to deployment in production. This Bidder must sign off on the software or system before its release, assist with closing any unfixed security issues and review the system's threat models to ensure that all possible avenues of attack have been secured.

3 Components of Scope

- 3.1 The scope and delivery time frame of each assessment shall be agreed to prior to commencement of the work. The scope may include remediation, recommendations, and extensive reporting. The bidder is required, at SARS discretion, to offer the following services:

- 3.1.2 Software security - Eradicating software vulnerabilities before a product's release is crucial to SARS software development. Bidders are to refer to Figure 1 below. SARS is looking for a Bidder in the provision of comprehensive application security verification, illustrated in the top right of the quadrant. The service Bidder is required to verify all security mechanisms and vulnerabilities based on threat analysis using manual penetration testing or code review or both.
- 3.1.3 Bidders must note that SARS is not looking for external application scanning services or auto source code tool based services in this RFP. The Bidder will employ methods that match the prevailing threat landscape and is expected to stay ahead of emerging threats and trends.

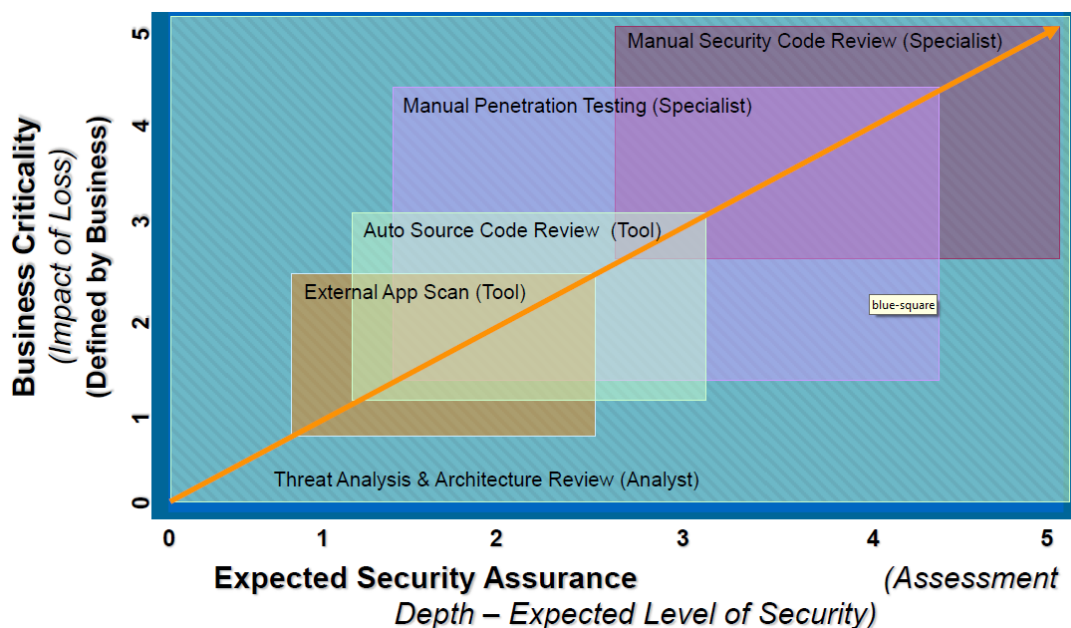


Figure 1.

- 3.1.4 Red Team exercise - the Bidder will be required to provide world class hacking expertise to help SARS security teams follow the entire attack lifecycle carried out by sophisticated, persistent attackers. Typically in this exercise, SARS defenders (Blue Team) receive little or no information at the beginning of the assessment, as a Red Team is supposed to emulate a real, targeted attack. The goals and framework conditions of such a test are agreed in advance between the Bidder and SARS. A coordinated ethical approach should have priority over the effectiveness of attack techniques, but it is often in tension with methods used by real attackers.
- 3.1.5 Purple Team exercise – The Purple Team exercise is a collaborative approach combining the Red and Blue Teams' (SARS defenders) efforts in an interactive setting by performing different real-world attack scenarios, while the Blue Team is actively watching which elements are not detected. Afterwards, both the Blue team and the Red team improve their approaches and retry.

- 3.1.6 The Bidder at SARS discretion may be required to provide expert digital forensics services and remediation in case of a cyber breach.
- 3.1.7 Threat analysis – assisting SARS to develop use cases that can be implemented in the Security Operation Center (SOC) monitoring environment which will contribute to improved monitoring and security posture.
- 3.1.8 The Bidder will employ methods that match the prevailing threat landscape and is expected to stay ahead of emerging threats and trends.

4 UNDERLYING PRINCIPLES TOWARDS RFP

4.1 Capability

- 4.1.1 There are a few certifications for both the analysts and industry players. The Bidder is required to demonstrate that they have some industry related certifications such as Certified Information Systems Security Professional (CISSP), Council for Registered Ethical Security Testers (CREST), Certified Ethical Hacker (CEH), including, Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE), Offensive Security Web Expert (OSWE), Offensive Security Wireless Professional (OSWP), Offensive Security Exploitation Expert (OSEE), Offensive Security Experienced Penetration Tester (OSEP), Payment Card Industry Data Security Standard (PCI DSS) and ISO certifications for analysts and as well as those applicable for the Bidder' organisation.
- 4.1.2 The Bidder must make use of resources resident within the Republic of South Africa and may not outsource the provision of services to external 3rd parties without prior written consent from SARS.
- 4.1.3 The Bidder must be able to demonstrate that they play an active role in the industry through reputable research or tools published or conferences presented. Additionally the Bidder may be required to supply contactable client references, details of the actual work conducted is not a requirement.
- 4.1.4 Bidder to provide SARS with a breakdown of different assessments they provide and examples of the report outputs from the assessment.
- 4.1.5 Supplier to provide SARS with analysts Curriculum Vitae's (CV) / Resume indicating the experience, personal identifiable information may be anonymised.
- 4.1.6 Supplier to provide SARS with a dedicated client service person to manage the business interactions.
- 4.1.7 The bidder's staff assigned to SARS will be required to meet specific security vetting criteria as defined by SARS.

5 SECURITY PROCESS

- 5.1 Security vetting and clearance of all relevant staff prior to commencement of jobs under embargo.
- 5.2 The Bidder staff assigned to SARS assessments must sign the Oath of Secrecy form and be familiar with applicable SARS internal policies prior to commencement of work.
- 5.3 In the course of the assessments, analysts may be assigned SARS equipment and access privileges where applicable. Usage of the equipment and access provided is governed by SARS Information Security Policies.
- 5.4 The Bidder must not retain any SARS data or information that they may come across in the conduct of their work. The bidder must certify that they have disposed of the data in accordance with SARS Records Management - Internal Policy.