Quality Council for Trades & Occupations
www.qcto.org.za
256 Glyn Street, Hatfield, Pretoria, 0083
Private Bag X278, Pretoria, 0001
+27 12 003 1800

TERMS OF REFERENCE (TOR): SUPPLY LICENSES, INSTALL, CONFIGURE AND SUPPORT A VULNERABILITY ASSESSMENT TOOL (NESSUS OR EQUIVALENT) FOR 24 MONTHS

1. INTRODUCTION

The QCTO is a Schedule 3A Public Entity that was established in accordance with the Skills Development Act, No. 97 of 1998 (as amended) and the National Qualifications Framework Act, No. 67 of 2008 (as amended) and came into operation on 1 April 2010. The main functions of the QCTO, amongst others, are to develop standards for occupational qualifications, including trades and skills programs, to accredit skills development providers and assessment centres, to conduct assessments, quality assurance and issue certificates to qualifying candidates.

Therefore, the QCTO is responsible for standards generation and maintenance; quality assurance of occupational full and part qualifications registered on the National Qualifications Framework (NQF) and the Occupational Qualifications Sub-Framework (OQSF) policy, including skills programs.

The QCTO has approximately +-160 staff members and is situated in Hatfield, Pretoria. The ICT unit comprises five (5) technicians responsible for the organisation's IT infrastructure and security. More information can be obtained from https://www.qcto.org.za

2. AIM

This RFQ aims to appoint a suitable service provider to supply licenses, install, configure, implement, and support a vulnerability assessment tool (Nessus Professional or an equivalent industry-recognised solution). The QCTO, through this solution, aims to conduct monthly internal vulnerability assessments and penetration testing to proactively identify, remediate, and manage security weaknesses within its IT environment, reducing reliance on costly annual external tests.

3. SCOPE OF WORK AND DELIVERABLES

The appointed service provider will deliver on the following:

3.1. Supply a perpetual or subscription-based license for a vulnerability assessment tool (Nessus Expert or equivalent) for a period of 24 months with advanced support.

3.2. Install, configure, and implement the vulnerability assessment tool on the QCTO's designated server or workstation, ensuring compatibility with the existing IT environment (Windows Server, Windows 10/11 endpoints, network devices, firewalls, and web applications).

3.3. Configure the tool to allow scanning of up to five (5) concurrent authenticated and unauthenticated vulnerability scans across the QCTO network, covering a maximum of 500 IP addresses or assets.

3.4. Ensure the tool provides the following capabilities:

- Network vulnerability scanning (internal and external)
- Web application scanning
- Configuration and compliance scanning (e.g., against NIST, MISS standards)
- Authenticated and unauthenticated scanning options
- Asset discovery and inventory
- Customisable scan templates and policies
- Scheduled and on-demand scanning

3.5. Configure the tool to generate detailed vulnerability reports, including:

- Executive summaries
- Technical findings with severity ratings (Critical, High, Medium, Low)
- Remediation recommendations and steps
- Trend analysis and historical reporting

3.6. Integrate the tool with the QCTO's existing email system to automatically notify the five (5) ICT technicians of scan results and critical findings.

3.7. Provide user access for up to five (5) designated ICT technicians, with role-based access controls (e.g., Administrator, Scanner, Reader).

3.8. Provide end-user training for the five (5) ICT technicians on the following:

- Installing and configuring the tool
- Creating and scheduling scans
- Interpreting scan results
- Generating and exporting reports
- Remediation guidance

3.9. Provide administrator training for two (2) designated users on advanced features, custom policies, and troubleshooting.

3.10. Provide ongoing technical support and maintenance for the duration of the contract (24 months).

3.11 The service provider shall conduct an initial assessment of the QCTO environment prior to installation to ensure compatibility and a draft remediation plan after.

4. TRAINING

4.1. The successful bidder must train the specified QCTO officials (five ICT technicians) after implementing the solution.

4.2. Training must include:

- Hands-on practical sessions using the QCTO's own environment

- Comprehensive training manuals and user guides
- Recorded training sessions for future reference

4.3. A certificate of completion shall be issued to each trained official.

5. PROJECT TIMELINE

5.1. The successful bidder must be able to supply, configure, and install the required services within four (4) weeks of receiving the purchase order.

5.2. The proposed project timeline should include the following milestones:

- Week 1: Environment assessment and compatibility check
- Week 2: Installation and basic configuration
- Week 3: Advanced configuration, policy creation, and testing
- Week 4: User training, administrator training, and go-live

6. EVALUATION CRITERIA

Stage	Criteria
1	Detailed CVs of the key personnel assigned to the project At least one team member must hold an active, industry-recognised technical certification, specifically OSCP (Offensive Security Certified Professional), and one of CEH (Certified Ethical Hacker) or CompTIA PenTestPlus(+). A copy of the Certificates will be acceptable as proof.
2	At least three (3) signed and dated reference letters from similar projects completed in the last three (3) years

7. ENQUIRIES

7.1 For further information, please contact the following QCTO staff members:

Technical enquiries can be directed to:

Mr Hangwelani Tshifaro
Tel no: 012 003 1829
Email: Tshifaro.h@qcto.org.za

Ms Nyeleti Maluleke
Tel no: 012 003 1856
Email: Maluleke.n@qcto.org.za