REQUEST FOR QUOTATION (RFQ)

RFQ2025/ 129: Appointment of a service provider to conduct Application Penetration Testing Services for an Enterprise System

Contents

Contact person: **Philani Khatheni email - PhilaniK2@dut.ac.za**

Technical queries: **cio@dut.ac.za**

Closing date for submission of bids: **05 December 2025 by 11am**

Bids must be submitted on one (1) email (zip folder or WeTransfer) to roq@dut.ac.za

NB: Bids submitted to any other email will not be accepted.

1. Introduction

Durban university of Technology hereby invites suitably qualified, accredited, and experienced cybersecurity service providers to submit quotations for conducting Application Penetration Testing on a mission-critical enterprise application scheduled for go-live. The objective is to identify vulnerabilities, misconfigurations, and security gaps that could compromise data confidentiality, integrity, and availability.

2. Background & Context

The institution is preparing to deploy a major enterprise application that supports core business operations and processes. In line with corporate governance, POPIA compliance, IT security standards, and audit requirements, the institution must ensure that the application is tested for security weaknesses before go-live.

The penetration test must evaluate the application against industry frameworks and best practices, including the OWASP Top 10, NIST SP 800-115, ISO/IEC 27001, and relevant regulatory obligations.

3. Scope of Work

The appointed service provider will be required to perform a comprehensive, manual-led and tool-assisted Application Penetration Test covering, at minimum, the following areas:

3.1 Application Security Assessments

- Authentication and session management
- Authorization and access control
- Input validation and injection vulnerabilities
- Insecure Direct Object References (IDOR)
- Cross-Site Scripting (XSS)
- SQL/NoSQL/Command Injection
- Business logic flaws
- API security and endpoint testing
- File upload and download controls
- Error/exception handling
- Data protection and encryption controls

3.2 System & Architecture Review

- Review of environments (Development, UAT, Production)
- Assessment of integrations (API, middleware, microservices, databases)
- Review of network exposure and open ports related to the application

- Testing of application server configurations

3.3 Compliance & Governance

- POPIA compliance assessment
- Data exposure and leakage risks
- Alignment to institutional cybersecurity policies

4. Deliverables

The service provider must deliver:

4.1 Detailed Penetration Testing Report (Mandatory)

Executive summary (non-technical)

Summary risk heatmap

- Detailed findings with:
- Vulnerability description
- Evidence/screenshots
- Impact assessment
- Likelihood and severity classification
- Risk rating in line with OWASP/NIST
- Clear, practical remediation recommendations
- Root cause analysis for critical/high findings

4.2 Validation & Retesting Report

- Confirmed closure of issues
- Updated risk rating post-remediation

4.3 Debriefing Presentation

- Technical walkthrough with ICTS/security teams
- Executive briefing to Management/Steering Committee

5. Service Provider Requirements

Service providers must meet the following minimum criteria:

- At least 5 years' experience delivering penetration testing for enterprise systems
- Qualified and certified testers (minimum OSCP, CEH, CISSP, GIAC or equivalent)
- Experience in testing ERP, SIS, HCM, financial systems, or equivalent enterprise applications

- Proof of accreditation or partnership with reputable cybersecurity bodies
- Demonstrated track record (minimum 3 references from the past 3 years)
- Ability to provide independent testing (no conflict of interest with application developers)

6. Project Duration & Timelines

Testing must commence immediately upon issuing the Purchase Order and be completed within:

- Testing window: 7–14 days
- Initial report: within 5 working days after assessment
- Retesting: within 5 working days after remediation

Urgent timelines apply due to scheduled application go-live deadlines.

7. Pricing Structure

The quotation must include a detailed cost breakdown:

- Penetration testing fee
- Reporting and validation
- Retesting costs
- Travel (if applicable)
- Total price including VAT

8. Evaluation Criteria

8.1 Compliance documents – Phase 1

- tax Clearance pin
- CIPC documents
- Signed Forms 5 to 8
- Completed pricing as per #7

Bidders must provide the above documents to be evaluated in Phase 2

8.2 Functionality (Minimum threshold: 70%)

Criteria	Sub points	Points
Company profile: • Background • Details on experience of the company related to the above scope of work (minimum 5 years' experience in penetration testing of ERP systems) • Details on previous projects where work was done for similar services • Proof of accreditation or partnership with reputable cybersecurity bodies • Confirmation of ability to provide independent testing (no conflict of interest with application developers)	2 point 4 points 4 points 3 points 2 points	15 points

Detailed Methodology & Approach with test plan as per above scope of work: • Detailed methodology that addresses the Scope of work • Methodology that partially addresses the scope of work	 30 points 20 points	30 points
Qualifications of Testing Team CVs with relevant certifications / qualifications must be submitted. **1. Project Manager:** • (Minimum 10 years' experience with project Management qualification in penetration testing for enterprise systems **2. Senior Technician or similar** • Minimum 7 years' experience in penetration testing for enterprise systems with relevant qualifications. 3. Organogram for this project which must include names, responsibility, job title:	 10 points 10 points 10 points	30 points

Three (3) signed letters of customer references that includes the following: • Customer letterhead with email address, phone number and is signed. • When the work was carried out (not older than 3 years) • If the work carried out was similar to the above scope of work.	1 point each 2 points each 2 points each	15 points
Project timeline and testing schedule which includes key milestones and timelines (refer # 6 above)		10 points
Bidders must obtain minimum 70 points to be evaluated in Phase 3		**100 points**

8.3 Evaluation of Price / B-BBEE (80/20)

Service providers are to submit a valid B-BBEE certificate – no submission will result in 0 points being awarded

Calculation of Price:

$$Ps = 80\left(1-\frac{(Pt - Pmin)}{Pmin}\right)$$

Where:

Ps = Points scored for price of tender under consideration Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender.

Calculation of B-BBEE points:

Specific Goal	**80/20**

		UP to R 50M	
		Sub-points	Total Points
	Exempted Micro Enterprise (EME) or Qualifying Small Enterprise (QSE)	3	3
Black-owned Enterprises	100% Black owned enterprise	3	3
	Minimum 51% black-owned enterprise	2	
	Minimum 25% black-owned enterprise	1	
Black Women owned Enterprise	100% Black Women owned enterprise	5	5
	Minimum 51% black women-owned enterprise	4	
	Minimum 25% bl ack women-owned enterprise	3	
	Less than 25% of black women-owned enterprises but not less than 10%	2	
Enterprise owned by Youth	100% Black Youth owned enterprise	5	5
	Minimum 51% black Youth owned enterprise	4	
	Minimum 25% black Youth owned enterprise	3	
	Below 25% black youth owned enterprises but not less than 10%	2	
Enterprises owned by people with disabilities	Minimum of 51% owned by people with disabilities	2	2
	Minimum of 10% owned by people with disabilities	1	
Additional Specific goals	An entity which is at least 51% owned by black people living in rural or underdeveloped areas or townships	1	1
	A cooperative which is at least 51% owned by black people	1	1
			20