



TERMS OF REFERENCE

SCM74/ICT/INFRASTRUCTURE/REVAMP/2026

APPOINTMENT OF A PROFESSIONAL SERVICE PROVIDER (PSP) / ICT CONSULTANT

1. BACKGROUND

The Performing Arts Centre of the Free State (PACOFS) hereby invites suitably qualified and experienced service providers to submit quotations for appointment as a Professional Service Provider (PSP) / ICT Consultant to support the implementation of the ICT Infrastructure Revamp Project.

The appointed consultant will be required to benchmark the current environment against relevant industry standards and best-practice frameworks (ISO/IEC 27001, the NIST Cybersecurity Framework, CIS Controls, and POPIA / other applicable data protection legislation).

2. SCOPE OF WORK

The appointed consultant will be required to perform the following, at minimum:

2.1 IT Infrastructure Assessment

- Review of servers (physical and virtual), storage, backup systems and the data centre / server room environment;
- Review of hardware lifecycle, capacity, redundancy and disaster recovery / business continuity arrangements;
- Assessment of cloud infrastructure and services in use (if applicable), including configuration and cost-efficiency;
- Review of software licensing, patch management and endpoint management practices;

2.2 Network Assessment

- Review of network architecture, topology and segmentation (LAN, WAN, Wi-Fi, VPN, remote access);
- Assessment of network hardware (routers, switches, firewalls, load balancers), including configuration and lifecycle;
- Bandwidth, performance, availability and redundancy review;
- Review of network monitoring, logging and management tools; and
- Identification of single points of failure and resilience gaps.

2.3 Cybersecurity Assessment

- Vulnerability assessment of network, systems, applications and endpoints;
- Review of identity and access management, privileged account management and authentication controls;
- Review of perimeter and endpoint security controls (firewalls, anti-malware, EDR/XDR, email and web filtering);
- Assessment of data protection, encryption and data loss prevention practices, with reference to applicable data protection legislation;
- Review of security policies, procedures, the incident response plan and user awareness practices;
- Review of third-party / vendor access and supply-chain security risk; and
- Non-intrusive penetration testing / controlled vulnerability scanning of a defined scope, subject to written authorisation and a signed rules-of-engagement document.

2.4 Recommendations and Reporting

- A consolidated findings report covering infrastructure, network and cybersecurity, with risk ratings (critical / high / medium / low);
- A prioritised, practical remediation roadmap with indicative timelines, effort and budgetary cost estimates;
- A gap analysis against the chosen best-practice framework(s); and
- An executive summary suitable for presentation to PACOFS's management / board.

2.5 Support with Follow-on RFQ

- Assist PACOFS in developing the scope of work, technical specifications and evaluation criteria for a subsequent RFQ to implement the recommended remediation and improvement projects;
- Provide input on realistic budget ranges and delivery timelines to support PACOFS's procurement planning; and
- Review draft RFQ documentation prepared by PACOFS and provide written comment prior to issue.

3. KEY DELIVERABLES

No.	Deliverable
1	Inception report and detailed project mobilisation plan
2	Finalised technical specifications, scope of work and bid/tender documentation for the procurement phase
3	Vendor engagement support and bid evaluation assistance
4	Deployment oversight (hardware, network, fibre, cloud migration, security implementation)
5	Project close out report

4. MINIMUM REQUIREMENTS FOR BIDDERS

- Registered and active on the Central Supplier Database (CSD);
- The bidding entity and/or its proposed lead project manager must hold current, valid membership or registration with a recognised professional body relevant to the services offered – IITPSA (Institute of Information Technology Professionals South Africa) for ICT practitioners, and/or PMSA or PMI for project management professionals. Proof must be submitted as a valid membership certificate or letter of good standing, current as at the closing date of this RFQ;
- A minimum of five (5) years' demonstrable experience delivering ICT infrastructure assessment projects of comparable scope (cloud migration, networking, cybersecurity, data centre / fibre infrastructure);
- Relevant professional certifications for proposed team members (CISSP, CISM, CEH, OSCP, CompTIA Security+, ISO/IEC 27001 / Cisco / network certifications, as applicable to the role performed);
- A valid Tax Compliance Status PIN / Tax Clearance Certificate;
- Company registration documents (CIPC) and a valid B-BBEE certificate or sworn affidavit (for EMEs/QSEs);
- At least three (3) contactable references from similar projects completed in the past five years;
- Proof of current professional indemnity insurance and cyber liability insurance, reflecting the insured party's name (matching the bidding entity), insurer, indemnity limit, cover type and a validity period extending through the full engagement period;
- A signed confidentiality / non-disclosure undertaking;
- A technical proposal addressing the scope of work, including proposed methodology, tools and project plan; and
- CVs and certifications of proposed team members.

5. PRICING SCHEDULE (ANNEXURE A)

Bidders must complete the table below. All prices must be quoted in South African Rand (ZAR), VAT exclusive and VAT inclusive, and must be all-inclusive of travel, tools/licensing and disbursements unless otherwise stated.

Item / Deliverable	Unit	Qty	Unit Price	Total
IT Infrastructure Assessment				
Network Assessment				
Cybersecurity Assessment (incl. vulnerability scan / penetration test)				
Consolidated Report & Remediation Roadmap				
Executive Presentation				
Support with Follow-on RFQ Development				
Other / Disbursements (specify)				
Subtotal (excl. VAT)				

Item / Deliverable	Unit	Qty	Unit Price	Total
VAT				
Total (incl. VAT)				

6. EVALUATION CRITERIA

Phase 1: Compulsory Documents

- Proof of registration with the Central Supplier Database (CSD);
- Completed and signed SBD forms (SBD 4 and SBD 6.1);
- A detailed company profile, clearly stipulating the relevant experience, knowledge and directorships of the company; and
- Valid B-BBEE certification or affidavit to claim specific goals in terms of SBD 6.1 (*non-submission will not disqualify the quotation*).

NB: Failure to submit the above-mentioned documents will lead to disqualification.

Phase 2: Evaluation Criteria (Functionality)

Bids will be evaluated on compliance and functionality. Bidders that score a minimum total of 70 points for the functionality evaluation will be evaluated using the 80/20 system in terms of Regulation 4(1) of the Preferential Procurement Regulations (PPR), 2022, where a maximum of 80 points is allocated for price and a maximum of 20 points is allocated for PACOFS's specific goals.

Criterion	Description	Points
B1: Company Experience of Project Team	Relevant experience and track record on comparable ICT infrastructure / cybersecurity assessments in the public sector. Provide <u>reference letters</u> from previous clients for the provision of infrastructure / cybersecurity assessments in the public sector. The reference letter(s) should be on the letterhead of the serviced client and should reflect at least the client's name, a full description of the service rendered, and a contact person with contact details. Letters must be authorised. 5 points awarded for each valid reference letter (maximum 30 points).	30
B2: Methodology and Project Understanding	All bidders are required to submit a detailed methodology covering the project objectives, scope of work and deliverables, with a detailed explanation of how supervision of the work will be carried out, and the tools and resources to be used for the entire project life cycle. The methodology must demonstrate the relevance and suitability of the tools and processes used to ensure quality control and assurance in all phases of the project. The methodology must demonstrate project understanding through the following five (5) components: • Project objectives. • Scope of work and deliverables. • A detailed explanation of how supervision of the work will be carried out. • Tools and resources to be used for the entire project life cycle. • Relevance and suitability of tools and processes to ensure quality control and assurance in all phases of the project.	25

Criterion	Description	Points
	Scoring: • Method statement inclusive of all 5 components = 25 points • Method statement inclusive of 4 components = 20 points • Method statement inclusive of 3 components = 15 points • Method statement inclusive of 2 components = 10 points • Method statement inclusive of 1 component = 5 point • No submission = 0 points <i>The evaluator must be able to identify the 5 components that guide understanding of the project.</i>	
B3: Qualification, Certification and Experience	Qualifications of the members who will form part of the team, if appointed. Certified copies of qualifications must be provided. Proposed project team – minimum requirements per role: ICT Project Manager / Lead Consultant • Relevant ICT Degree qualification • AZURE Administrator Certified • Cisco Certified Network Professional (CCNP) • Linux Certified • MCSE Certified or Similar to Microsoft • Project management experience • Minimum 5 years' ICT consulting experience • Demonstrated ICT infrastructure assessment experience Cybersecurity Specialist • Relevant ICT Degree qualification and cybersecurity / information security qualification • Recognised cybersecurity certification(s), where applicable • Experience with ISO 27001 / NIST / CIS • Cybersecurity assessment experience • Minimum 5 years' ICT consulting experience ICT Infrastructure Architect • ICT Degree qualification • Project Management Certificate • Enterprise network architecture • Azure Administrator Certified Certificate • Cloud infrastructure • Microsoft 365 • Infrastructure modernisation • Minimum 5 years' ICT consulting experience ICT Governance / Risk Specialist • ICT Degree qualification • Itil Certified Certificate • ICT governance proven experience • Risk management • ICT Audit Experience • Compliance • Public-sector governance <i>The bidder may propose additional specialists where required.</i>	25

Criterion	Description	Points
B4: Work Plan	Detailed programme of works and associated project cash flow. For the programme and cash flow, the following five (5) components must be stated in writing and/or be visible on a programme and cash-flow spreadsheet: • Milestones. • Critical path. • Resource allocation. • Task dependency map. • Monthly project cash flow (which must be in line with the project cost and programme of works). <i>The bidder must clearly show all five components in the submission (a Microsoft Project visual illustration alone is not sufficient).</i> Scoring: • Work plan inclusive of all 5 components = 20 points • Work plan inclusive of 4 components = 15 points • Work plan inclusive of 3 components = 10 points • Work plan inclusive of 2 components = 7 points • Work plan inclusive of 1 component = 5 point • No work plan / cash flow submitted = 0 points	20
TOTAL	Bidders must score a minimum of 70 points to be considered for further evaluation.	100

Note: A bidder that scores less than 70 points out of 100 as per categories in respect of functionality will be regarded as submitting a non-responsive proposal and will be disqualified.

Phase 3: Price and Specific Goals

Bidders who meet the minimum functionality score of 70 points will proceed to Phase 3, where the maximum points for this RFQ are allocated as follows:

	Points
Price	80
Specific goals (as per SBD 6.1)	20
Total points for price and specific goals	100

7. TAX COMPLIANCE

Where the recommended bidder is non-tax compliant, the bidder will be given seven (7) days to rectify their tax status, failing which the bid will be disqualified.

In terms of National Treasury Instruction No. 4A of 2016/2017 regarding the Central Supplier Database (CSD), all bidders must register on the CSD, which will be used to verify the following information:

- Business registration, including details of directorship and membership;
- Bank account holder information;

- In the service of the State status;
- Tax compliance status;
- Identity number; and
- Tender default and restriction status.

8. TENDER DEFAULTERS AND RESTRICTED SUPPLIERS

No award shall be made to a bidder whose name (or the name of any of its members, directors, partners or trustees) appears on the National Treasury's Register of Tender Defaulters, or who has been placed on the National Treasury's List of Restricted Suppliers. PACOFS reserves the right to withdraw an award, or to cancel a contract concluded with a bidder, should it be established at any time that the bidder has been blacklisted by National Treasury or another government institution.

9. OUT CLAUSE

PACOFS reserves the right not to appoint any service provider. PACOFS does not bind itself to accept either the lowest price or any other bid, and reserves the right to accept the bid it deems to be in the best interest of the entity.

10. VALIDITY PERIOD

Quotations must remain valid for a period of 30 days from the closing date.

11. SUBMISSION AND CLOSING DATE

11.1 Quotations must be submitted by email to quotation@pacofs.co.za not later than **07 October 2026**. Hand-delivered documents will not be accepted.

11.2 The closing date is 07 October 2026.

Please note: *No late submissions will be considered.*

12. ENQUIRIES

For more information, please contact the SCM Department at quotation@pacofs.co.za or 051 447 7771 ext. 2234.

13. PERIOD

Contract Period 1 Year service level agreement.

CLOSING DATE FOR SUBMISSION OF THE BID

WEDNESDAY, 07 OCTOBER 2026 – 11:00

No late submissions will be considered.

ANNEXURE B: PROPOSED PROJECT TEAM – QUALIFICATIONS, CERTIFICATIONS AND EXPERIENCE (CRITERION B3)

In response to Criterion B3 (Qualification, Certification and Experience), the bidder proposes the following project team, in line with the minimum role requirements set out under Section 4 above. The bidder must insert the actual name of each proposed team member and attach certified copies of qualifications and certifications, together with a full CV, for every individual listed. Additional specialists may be proposed where required for the scope of work.

Note: Fields marked “[To be completed by bidder]” must be populated with the real name and CV reference of the individual being put forward. Do not submit this table with placeholder text.

Proposed Role	Name of Team Member	Minimum Requirements	Relevant Certification(s)
ICT Project Manager / Lead Consultant	<i>[To be completed by bidder]</i>	- Relevant ICT qualification - Project management experience - Minimum 5 years' ICT consulting experience - Demonstrated ICT infrastructure assessment experience	—
Cybersecurity Specialist	<i>[To be completed by bidder]</i>	- Relevant cybersecurity / information security qualification - Recognised cybersecurity certification(s), where applicable - Experience with ISO 27001 / NIST / CIS - Cybersecurity assessment experience	e.g. CISSP, CISM, CEH, OSCP, CompTIA Security+ (as applicable)
ICT Infrastructure Architect	<i>[To be completed by bidder]</i>	- Enterprise network architecture - Server infrastructure - Cloud infrastructure - Microsoft 365 - Infrastructure modernisation	Relevant vendor / architecture certification (e.g. Cisco, Microsoft, VMware), as applicable
ICT Governance / Risk Specialist	<i>[To be completed by bidder]</i>	- COBIT - ICT governance - Risk management - Audit - Compliance - Public-sector governance	COBIT certification / ISO 27001 Lead Auditor, as applicable

The bidder confirms that certified copies of qualifications and certifications, and full CVs, for each named team member above are attached as supporting documentation to this bid, in compliance with the requirements of Criterion B3 and Section 4 of this RFQ.