International Trade Administration Commission of South Africa

TERMS OF REFERENCE FOR THE APPOINTMENT OF A PANEL OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SERVICE PROVIDERS FOR THE INTERNATIONAL TRADE ADMINISTRATION COMMISSION OF SOUTH AFRICA FOR A PERIOD OF 36 MONTHS

RFP NUMBER: ITAC 03-2025/2026

Date Issued: 28 January 2026

Closing date and time: 27 February 2026 at 11:00

Bid Validity Period: 120 days

TENDER BOX ADDRESS:

The **dtic** Campus
Ground Floor, Block E
77 Meintjies Street
Sunnyside
Pretoria
0002

TABLE OF CONTENTS

1. Purpose

The purpose of this Request for Proposal (RFP) is to solicit proposals from suitably qualified and experienced service providers to serve on a panel of ICT service providers for ITAC.

This RFP does not constitute an offer to do business with ITAC but merely serves as an invitation to bidder(s) to facilitate a requirements-based decision process.

2. Background

2.1 Establishment of the International Trade Administration Commission (ITAC)

The International Trade Administration Commission (ITAC) was established in terms of Section 7 of International Trade Administration Act, 2002 (Act No. 71 of 2002).

ITAC was established with its own offices located in Tshwane, Sunnyside at ***the dtic*** campus in 2003. The current organisational structure provides for the employment of 131 employees. The said structure consists of Senior Management Service (SMS); Middle Management Service (MMS) and other employees.

2.2 ITAC's Key Strategic Objectives

To achieve its aims, ITAC has identified the following strategic objectives to guide its operations, namely to:

2.2.1 Promote industrialisation.

2.2.2 Promote transformation.

2.2.3 Conduct distributional impact assessments of trade measures affecting consumers' welfare and downstream industries.

2.2.4 Ensure efficient administration of trade instruments (customs tariff investigations, trade remedies, import and export control.

2.2.5 Monitoring, evaluation and modernisation of administrative and operational processes.

2.3 Functional Areas of ITAC

There are two main functional areas for ITAC with supporting business units reporting there under, namely:

2.3.1 Core business

- Tariff Investigations.
- Trade Remedies.
- Import and Export Control.

2.3.2 Business Support Services

- Human Resources.
- Finance & Supply Chain Management.
- Communication Services.
- Information Technology.
- Internal Audit services.
- Legal Services.
- Policy and Research.
- Secretariat.
- Risk Management.

2.3.3 The Commission of ITAC

As compared to the other public entities in South Africa, ITAC has no Board of Directors but a Commission. The membership of the Commission is comprised as follows:

- Full time Chief Commissioner (CEO of ITAC).
- Full time Deputy Chief Commissioner.
- Part-time Commissioners (up to 10).

3. Project objective

To enable ITAC to achieve its mandate and strategic objectives, the services of suitably qualified and experienced service providers are required to serve on a panel of ICT service providers to provide a range of ICT services to ITAC.

The primary objectives of the service required are as follows: Acquisition

To streamline its procurement processes, ITAC aims to appoint a panel of service providers to provide a range of ICT services for a period of 36 months. Services will be sourced from the appointed competent service providers in line with the submitted proposals.
ITAC embarked on a digital transformation journey that aims to implement advanced technology to fulfil its mandate and for effective and efficient service delivery.

Bidders may submit proposals in respect of any or a combination of the following five (5) service categories:
3.1 Cyber Security services.
3.2 Server infrastructure services.
3.3. Cloud technology services.
3.4 Back-up and disaster recovery services.
3.5. Network and network security services.

4. Project Requirements and Deliverables

Below is a summary of ITAC's ICT Environment for each domain:

Cloud Environment

- Microsoft 365 E3 (130 licenses; roughly 120 active users)
- Hybrid enrolment (AD sync between on-prem and cloud)
- Cloud-native applications:
  - ManageEngine Service Desk & Endpoint Central
  - Mimecast Email Security Gateway
  - Symantec Security Cloud and AD Threat Defence
  - Sage 300 People (HR and Payroll)
- No custom workloads currently in the cloud

- **Planned upgrade:** adoption of **Azure subscription** for replication of on-prem Hyper-V VMs to Azure for resilience and DR

Server Infrastructure

- 3 physical servers running Hyper-V
  - 2 primary application servers replicating to the third server (backup node)
- No regional offices – single site located at **−25.7500907, 28.2001865** (Pretoria)

Network Environment

- 500 Mbps Internet line (bundled with managed firewall contract)
- Managed LAN services (ongoing contract)

Security Environment

- FortiGate 100F Firewall
- Symantec Endpoint Protection (Managed EDR)
- Symantec Active Directory Threat Defence
- Mimecast (Email Security and Archiving)
- Microsoft BitLocker (Disk Encryption)
- Microsoft LAPS (Local Admin Password Management)

Backup Environment

- **Commvault** for on-prem servers
- **Metallic (Commvault)** for laptops and M365 backups

The panel of service providers will be required to provide the following ICT services:

4.1 Cyber Security services

The appointed service provider(s) shall deliver expert advisory, implementation of various cybersecurity solutions, monitoring and management services across cybersecurity domains to strengthen ITAC's overall security posture. This includes establishing or supporting a formal Cybersecurity Response Team (CRT), reviewing and enhancing ITAC's cybersecurity framework, and operationalising cybersecurity controls across infrastructure, cloud and network domains.

Services must align with ITAC's enterprise risk profile and business objectives, with particular attention to governance, risk and compliance (GRC) practices, threat lifecycle management and incident response readiness.:

Key Deliverables

4.1.1 Cybersecurity Governance & Framework Review

- Conduct a baseline-assessment of ITAC's current cybersecurity maturity (policies, roles, tools, controls, supplier ecosystem).
- Assist ITAC in performing third party risk assessment
- Review or develop a cybersecurity framework aligned to NIST CSF 2.0 (functions: Govern, Identify, Protect, Detect, Respond, Recover)
- Define roles, responsibilities, accountability including oversight mechanisms (board, senior management, CRT, suppliers) in line with the new "Govern" function of CSF 2.0
- Provide policy template(s) and a roadmap to align governance, risk management and compliance (GRC) with cybersecurity strategy.

4.1.2 Cybersecurity Response Team (CRT) Establishment & Support

- Define the CRT composition.
- Provide training and playbooks for CRT activation, forensic triage, legal/regulatory reporting, internal/external communications.
- Support periodic 'table-top' incident response exercises and full live incident simulations.

4.1.3 Threat Management & Monitoring

- Implement or support continuous threat detection, monitoring, logging, and incident triage services (e.g., Security Information & Event Management (SIEM), SOC, Endpoint Detection & Response (EDR), Extended Detection & Response (XDR), threat-hunting, SASE, DLP, Firewall).
- Define key metrics (e.g., mean time to detection, time to containment, number of incidents by severity) and report monthly.

4.1.4 Protection Controls

- Review and advise on security architecture across network, cloud, identity/access management, data encryption, zero-trust concepts (least-privilege etc), secure configuration and patch-management.
- Support in defining or refining incident management/response processes (aligned with the "Respond" function) including escalation, communication, remediation and lessons-learned cycles.

- Assist with establishing preventative controls (vulnerability scanning, penetration testing, red-team/blue-team exercises).
- Provide advisory in emerging technology domains (cloud native, hybrid infrastructure, IoT/OT if applicable) and assist in security control selection and cost-estimation.

4.1.5 Testing, Exercising & Continuous Improvement

- Conduct annual full incident simulation, bi-annual tabletop exercises and periodic supplier incident scenario reviews.
- Deliver reports with findings, gaps, remediation plans; assist ITAC in prioritising improvements and tracking progress.
- Facilitate maturity assessment and roadmap updates, e.g., aligning to future cyber maturity levels (e.g. NIST maturity scores).

4.1.6 Compliance, Reporting & Assurance

- Ensure cybersecurity services support compliance with applicable legislation/regulation (e.g., POPIA, Cybercrimes Act, sector-specific regulation) and align with industry best-practice standards (e.g., ISO/IEC 27001/27002, COBIT).
- Provide quarterly governance reports to senior management covering regulatory developments, incident summary statistics, and strategic recommendations.
- Provide annual assurance review of cybersecurity controls and framework alignment.

Service Performance Metrics

- Cybersecurity policy review/approval: within 60 days of contract start.
- Mean Time to Detect (MTTD): < 30 minutes.
- Mean Time to Contain (MTTC): < 2 hours.
- Incident response exercise completion: 100% of scheduled exercises per annum.
- Framework alignment maturity: continuous improvement aligned with maturity frameworks such as NIST maturity scores (baseline to be established).

Service Levels & Response Times

Severity	Impact Description	Initial Response Time
Severity 1 (Critical)	Major breach, C1 service disrupted, data exfiltration or regulatory breach	15 minutes
Severity 2 (High)	Major threat, C2 service impacted, significant attempted intrusion	30 minutes
Severity 3 (Medium)	Incident contained, non-critical systems, near-miss event	2 hours
Severity 4 (Low)	Routine event/monitoring, no immediate impact	8 business hours

* Response time = acknowledgement of issue and mobilisation of resources.

Governance & Best Practice Alignment

- The framework shall be aligned to NIST CSF 2.0 including the new Govern function (Govern, Identify, Protect, Detect, Respond, Recover) to emphasise that cybersecurity is part of enterprise risk management and boarder organizational governance.
- The provider shall support ITAC's Cyber Risk Governance through defined roles, reporting lines, steering committee involvement, continuous monitoring and risk-tolerance review.
- Cybersecurity strategy must be aligned with ITAC's business objectives, risk appetite, regulatory environment and third-party dependencies.
- Adoption of "Zero Trust" architecture and principles such as least privilege, identity governance etc.
- Supply chain risk management must be incorporated, assessing third party vendors, dependencies, incidents and attack-surface exposure.
- Continuous improvement: regular maturity assessments, benchmarking, risk-based prioritisation of controls, lessons-learned from incidents, and iterative enhancement of controls.
- Incident response preparedness: service providers to assist in the establishment, maintenance and exercising of the CRT, ensuring roles, responsibilities and communication channels are tested and matured.

4.2 Server infrastructure services

The appointed service provider(s) shall design, provision, configure, manage and support ITAC's server infrastructure services for on-premises and hybrid infrastructure. This includes, endpoint devices, physical and virtual servers, operating systems (Windows Server, Hyper-V), virtualisation platforms, Domain Controllers, software deployment and patching, MSSQL services, Microsoft 365 E3 Suite, high-availability, backup and restore integration, monitoring, alerting, capacity planning and infrastructure lifecycle management

Key Deliverables

- Baseline server infrastructure assessment: inventory of servers, virtual machines, OS versions, patching status (including endpoint devices), performance metrics, end-of-life hardware/VMs, licensing status.
- Architecture design: virtualisation strategy, on-premises vs cloud and hybrid mapping, domain controller architecture, high-availability design, storage/compute/network interface design.
- Implementation: server provisioning, configuration, OS hardening, Active Directory management, domain controller setup, software deployment, patch, asset management processes.
- Monitoring and alerting: proactive health monitoring, performance metrics dashboards, capacity planning alerts, utilisation forecasting, automated remediation where feasible.
- Security and hardening: ensure servers comply with security baseline (configuration, patching, anti-malware, privileged access management), and integrate with cybersecurity domain controls.
- Lifecycle management: hardware refresh planning, virtual machine lifecycle, cloud resource optimisation, decommissioning of end-of-life.
- Load-balancing and high-availability: design, deploy and maintain infrastructure to support critical services with minimal downtime.
- Backup and DR integration: ensure server infrastructure is integrated into backup and disaster recovery services (link with your improved DR domain).
- Documentation: server architecture diagrams, configuration baselines, patch/upgrade logs, capacity planning reports.

- Quarterly review & optimisation: reports with recommendations for performance, cost/sizing optimisation, and security gap closure.

Service Performance Metrics

- Server infrastructure availability: 99.9 % uptime.
- Patch non-compliance rate less than 5% for all endpoint devices.
- Quarterly server infrastructure report delivered within 10 business days before the end of the quarter.
- Time to provision new server (physical or virtual) in production: Virtual Machine < 8 hours | Physical Machine < 2 business days.

Service Levels & Response Times

Severity	Impact Description	Initial Response Time
Severity 1 (Critical)	Server infrastructure outage affecting C1 service or domain controller failure	30 minutes
Severity 2 (High)	High-impact server degradation or impending capacity/availability risk	60 minutes
Severity 3 (Medium)	Non-critical server issue (e.g., non-C1 workload)	4 business hours
Severity 4 (Low)	Routine requests, server provisioning, patch scheduling	Next business day

*Response time = acknowledgement of issue and mobilisation of resources.

Governance & Best Practice Alignment

- The service provider must adhere to ITIL best practice frameworks for IT Service Management (incident, problem, change, configuration, release management).
- Ensure configuration hardening baselines, patch management policies, secure virtualisation, least-privilege access, separation of duties.
- Infrastructure services must integrate into ITAC's overall governance, risk and compliance (GRC) framework, aligning server infrastructure with business-continuity, disaster recovery and cybersecurity.
- Service provider to participate in quarterly governance reviews and produce executive reports for senior management.

4.3 Cloud technology services

The appointed service provider(s) shall assist ITAC in designing, migrating (if required), operating, optimising and securing cloud-based technology services. This covers infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), disaster-recovery-as-a-service (DRAAS) governance, cost management, licensing and operational support. The provider must partner with ITAC to develop the cloud adoption roadmap and governance framework.

Key Deliverables

- Cloud readiness assessment: current state, gaps, security posture, cost drivers, compliance risks.
- Cloud architecture design: reference architecture, landing zones, networking, identity & access management (IAM), data protection, hybrid connectivity, backup/DR linkages.
- Cloud governance framework: policies for resource provisioning, cost management, data security, access.
- Cloud security services: data encryption, IAM governance, continuous monitoring, log management, vulnerability scanning, cloud-native security tools.
- Cost optimisation and monitoring: resource use analysis, budget alerts, rightsizing.
- Cloud operations: patch management, service monitoring, backup/restore, incident response in cloud, vendor management of CSPs (cloud service providers).
- Implementation of hybrid or edge solutions as required by ITAC's environment: ensure seamless integration with on-premises, strict security and compliance controls.
- Reporting: monthly cost and usage dashboards, quarterly governance/security reports, annual maturity assessment.
- Training & knowledge transfer: upskilling internal staff on cloud operations, governance, and security.
- Cloud risk management: define third party cloud standards, risk assessment and report.

Service Performance Metrics

- Governance policy implementation: complete within first 90 days of contract start (baseline).
- IAM policy compliance: to be agreed.

- Cloud-security incidents: number of incidents reduced year on year.
- Cloud availability: 99.9 % uptime for critical cloud workloads.
- Quarterly cloud governance report delivered within 10 business before the end of the quarter.

Service Levels & Response Times

Severity	**Impact Description**	**Initial Response Time**
Severity 1 (Critical)	Critical cloud service outage, major data breach or compliance violation	30 minutes
Severity 2 (High)	Significant performance degradation of cloud services, or major security alert	60 minutes
Severity 3 (Medium)	Non-critical cloud service issue, or policy breach with no major impact	4 business hours
Severity 4 (Low)	Routine service request, cloud cost report, minor enhancement	Next business day

*Response time = acknowledgement of issue and mobilisation of resources.

Governance & Best-Practice Alignment

- Use recognised cloud governance frameworks.
- Ensure shared-responsibility model is understood for each cloud service, clearly define which controls are the responsibility of ITAC vs service provider vs cloud vendor.
- Monitor and optimise identity/access, data residency/privacy, cost, performance and business risk associated with cloud consumption.
- Continuous improvement: periodically review cloud architecture, security posture, cost-efficiency and organisational readiness.
- Integrate cloud services securely with on-premises and hybrid infrastructure.
- Leverage automation and orchestration to enforce governance controls.
- Reporting into governance/steering committees: monthly/quarterly reviews, alignment with ITAC’s enterprise risk appetite, regulatory compliance and business objectives.

4.4 Back-up and Disaster Recovery Services

The appointed service provider(s) shall design, implement, and maintain a comprehensive Back-up and Disaster Recovery (DR) framework aligned to ITAC’s approved Disaster Recovery Policy and Disaster Recovery Plan. Services must support ITAC’s Business Continuity Management System (BCMS) and ensure compliance with ISO 22301:2019, ISO/IEC 27001:2022, and COBIT 2019 DSS04. Providers shall participate in ITAC’s risk and audit reviews, maintain all recordkeeping aligned with the DR Policy, and support continuous improvement cycles in collaboration with the Risk Management and Audit Committee.

Key Deliverables

4.4.1 Disaster Recovery Governance

- Establish and support ITAC in maintaining a functional Disaster Recovery Team (DRT) with defined roles.
- Ensure all recovery activities align with RTOs/RPOs, Criticality 1 (C1) and Criticality 2 (C2) classifications.
- Provide templates and guidance for DR reporting, root-cause analysis, lessons-learned documentation, and continual improvement.

4.4.2 Backup and Replication

- Implement secure, encrypted, and immutable backup solutions across on-premises and cloud environments.
- Configure off-site replication in accordance with ITAC’s Backup & Restore Policy and validate backup job logs quarterly.
- Provide mechanisms for version control and retention compliant with POPIA and audit requirements.

4.4.3 Disaster Recovery Site Enablement

- Design, commission, or manage a secondary cloud DR site capable of hosting C1/C2 services, ensuring ≥ 99.9 % uptime.
- Establish replication or restore-from-backup procedures with automated failover where feasible.

4.4.4 Disaster Recovery Team Support

- Participate in DR Team activation, testing, and actual recoveries.
- Assist with the War Room setup, status dashboards, and stakeholder communication logs (per Annexures A–D of the DR Plan).

4.4.5 Testing and Exercises

- Conduct bi-annual DR simulation tests and quarterly backup recovery tests, in line with ISO 22301 Clause 8.5 and ITAC's annual DR test schedule.
- Document test plans, outcomes, deviations, and recommendations for inclusion in ITAC's DR Report.

4.4.6 Training and Awareness

- Provide annual role-specific training for DRT members and facilitate knowledge transfer to internal ICT staff.

4.4.7 Reporting and Continuous Improvement

- Submit quarterly Performance and Compliance Reports covering:
  - Backup success rates and restoration tests.
  - RTO/RPO achievement.
  - Outstanding risks and remediation actions.
- Compile a Post-Recovery Report after each activation or test, including cost impact and preventive actions.

Service Performance Metrics

Metric	Target	Reference
Backup Success Rate	≥ 98 % monthly	DR Plan
Restore Success Rate	100 % for tested datasets	DR Policy
DR Site Availability	≥ 99.9 %	DR Policy
Data Recovery Tests	Semi-annual	ISO 22301 8.5
Full DR Simulation	Annual (minimum)	ITAC DR Plan
DR Report Submission	Within 10 business days post-event	DR Plan
Compliance with POPIA & ISO 27001	100 %	DR Policy

Service Levels & Response Times

Severity	Impact Description	Initial Response Time
Severity 1 (Urgent)	Outage of C1 services / DR Site failure	30 minutes
Severity 2 (High)	Major degradation / partial loss of C2 services	60 minutes
Severity 3 (Medium)	Non-critical issues / deferred restores	8 business hours
Severity 4 (Low)	Routine service requests	Next business day

* Response time = acknowledgement of issue and mobilisation of resources.

Governance and Compliance Alignment

Service providers must adhere to and demonstrate competence in:

- Business Continuity Management Systems
- Information Security Controls
- COBIT 2019 DSS04 – Managed Continuity
- POPIA, Cybercrimes Act (19 of 2020), and ITAC's internal BCP & Incident Management Policies

4.5 Network and network security services

The appointed service provider(s) shall deliver design, implementation, operation and continuous-improvement services for ITAC's network infrastructure and associated network security controls. This includes the local area network (LAN), wide area network (WAN), wireless access, VPNs/remote access, network segmentation, firewalls, intrusion detection/prevention systems (IDS/IPS), network monitoring, and associated service levels. Services must cover the design, deploy, operate, optimise, and support.

Key Deliverables

- Baseline assessment of network topology.
- Network architecture design and documentation including logical and physical diagrams.

- Implementation of network security controls: firewalls, IDS/IPS, next-gen firewalls, web application firewalls (WAF) where applicable, zero-trust or least privilege segmentation. For example, segmentation to reduce lateral movement.
- Secure remote access solutions (VPN or secure access service edge SASE) including policies for remote/roaming users and endpoints.
- Network monitoring, logging, alerting (including network flow logs, traffic anomalies, DDoS mitigation) plus reporting dashboards.
- Patch management for network devices (switches, routers, firewalls) to ensure timely security updates.
- Performance and capacity management (throughput, latency, availability) plus proactive upgrades.
- Incident support: network security incident triage, root-cause analysis of network faults or security breaches, remediation.
- Documentation: network security policy, segmentation policy, access control policy, network topology register, device inventory audit logs.
- Periodic review and continuous improvement: recommendations for architecture improvements, security posture enhancements, network resilience (e.g. redundancy, high-availability, failover).

Service Performance Metrics

- Network availability: e.g., 99.9 % uptime for core network segments (to be agreed).
- Mean Time to Detect (network security events): < 1 hour.
- Mean Time to Restore (critical network outage or breach): < 4 hours.
- Proactive patch management and documentation.
- Number of network security incidents successfully contained per year (trend downward).
- Quarterly network security posture report delivered within 10 business days of quarter end.

Service Levels & Response Times

Severity	Impact Description	Initial Response Time*
Severity 1 (Critical)	Core network outage or major network security breach (C1 service impacted)	30 minutes
Severity 2 (High)	Major degradation of network performance, or significant security event but partial service impacted	60 minutes
Severity 3 (Medium)	Network segment issue (non-critical), minor security incident	4 business hours
Severity 4 (Low)	Routine change requests, monitoring alerts with no immediate impact	Next business day

*Response time = acknowledgement of issue and mobilisation of resources.

Governance & Best-Practice Alignment

- Align network security services with the CIA triad (Confidentiality, Integrity, Availability).
- Adopt “Zero Trust” network architecture: trust no user/device by default, segment and enforce least privilege.
- Maintain accurate network device inventory, configuration management, and patching.
- Incorporate network resilience, high-availability, redundant links, and failover controls consistent with business continuity planning.
- Ensure that participation in contract governance: regular review meetings, vendor performance KPIs, architecture change approvals, and security audits.
- Support regulatory compliance requirements: e.g., POPIA, Cybercrimes Act, sector specific obligations, with network security controls aligned accordingly.
- Encourage continuous improvement: perform network architecture reviews annually, adopt new technologies (e.g., SASE, SD-WAN) were business benefit evident.

NB: ITAC RESERVES THE RIGHT TO AMEND THE PROJECT DELIVERABLES WITHIN REASONABLE LIMITS AND CARE.

5. Service Speciality Offered / Covered

Bidders should tick the applicable service(s) which they are competent on:

Service Speciality Offered / Cover	**Tick**
Cyber Security services.	
Server infrastructure services.	
Cloud technology services.	
Back-up and disaster recovery services.	
Network and network security services.	

6. Expertise Required

During the evaluation of this project, the evaluation processes of ITAC will, *inter alia* consider the experience and credentials of the personnel proposed by the service providers on this project.

Please note that bidders must attach certified copies (not older than 3 months) of all required qualifications, relevant certificates, and copies of comprehensive and updated curricula vitae for each employee who will be utilised for this project.

7. Time Frames and Duration of Appointment

The envisaged appointment period will be 36 months.

8. Remuneration Condition

All claims for payment shall be submitted to ITAC monthly on condition that sufficient proof is submitted on progress made in respect of tangible deliverables, usable by ITAC, in terms of the project unless parties to the contract mutually decide and agree otherwise. ITAC's payment terms is 30 days from receipt of a valid invoice. No advance payments will be made by ITAC.

9. Contracting Process

The contracting between ITAC and the successful service provider shall come into effect upon receipt of the letter of appointment from ITAC and accompanied by a duly authorised copy of a purchase order from the Supply Chain Management Unit.

10. Special Provisions of Contract

Bidders are required to take note of the contents of the **Special Conditions of Contract**, which must be taken into consideration in preparing bid submissions and which shall form an integral part of the Contract Agreement between ITAC and the successful bidder.

10.1 The proposed total cost of the services must be clearly indicated stated in Annexure C: Pricing Schedule.

10.2 The proposal must clearly outline a detailed plan on how skills transfer will be done to the identified employees of ITAC.

10.3 The project and implementation plan must be included.

10.4 ITAC reserves the right to accept in whole or in part the proposal or to reject the proposal.

10.5 An overview of the project methodology to be used by the service provider must be provided.

10.6 Bidders must note that verification of the National Treasury Database of Restricted Suppliers and Register of Tender Defaulters will be conducted to ensure that ITAC does not enter into any contractual agreements with the restricted service providers.

11. General Conditions of Contract

Bidders are required to take note of the contents of the **General Conditions of Contract**, as contained under **Annexure A**, which shall form an integral part of the Contract Agreement between ITAC and the successful bidder.

Processing of the Bidder’s Personal Information

All Personal Information of the Bidder, its employees, representatives and associates (“Bidder Personal Information”) required under this RFP is collected and processed for the purpose of assessing the content of its tender proposal and awarding the bid. The Bidder is advised that Bidder Personal Information may be passed on to third parties to whom the Commission is compelled by law to provide such information. For example, where appropriate, the Commission is compelled to submit information to the National Treasury’s Database of Restricted Suppliers.

All Personal Information collected will be processed in accordance with POPIA and with the Commission’s Data Privacy Policy and Privacy Notices.

The following persons will have access to the Personal Information collected:

The Commission personnel participating in procurement/award procedures; and
Members of the public: within ten working days from the time the bid is awarded, the following information will have to be made available on the platforms that the bid was advertised on:

- contract description and bid number.
- names of the successful bidder(s) and preference points claimed.
- the contract price(s) (if possible).
- contract period.
- names of directors; and
- date of completion/award.

The Commission will ensure that the rights of the Bidder and of its employees and representatives (i.e. the right of access and the right to rectify) are effectively guaranteed in accordance with the procedures specified in the Commission’s PAIA manual.

In participating in this RFP, the Bidder consents to the use of its Personal Information for the purposes specified above.

12. Bidding Documents to be Completed, Signed and Submitted

All the information contained herein, specifically that under **Clauses 3 to 13**; as well as all the **Annexure B** must be considered and used as a basis for the formulation of proposals and preparation of cost estimates.

All the required information under **Annexure B**, and all the annexure thereto, must be duly and comprehensively completed and submitted.

12.1. Invitation to Bid (SBD 1).

12.2 Declaration of Interest (SBD 4).

12.3. Preference Points Claim Forms (SBD 6.1).

12.4. Service Level Agreement SLA / SBD 7.2 to be signed on appointment with the preferred service provider.

13. LEGISLATIVE FRAMEWORK OF THE BID

13.1 Tax Legislation

13.1.1 Bidder(s) must be tax compliant when submitting a proposal to International Trade Administration Commission of SA and remain compliant for the entire contract term with all applicable tax legislation, including but not limited to the Income Tax Act, 1962 (Act No. 58 of 1962) and Value Added Tax Act, 1991 (Act No. 89 of 1991).

13.1.2 It is a condition of this bid that the tax matters of the successful bidder be in order, or that satisfactory arrangements have been made with South African Revenue Service (SARS) to meet the bidder's tax obligations.

13.1.3 The Tax Compliance status requirements are also applicable to foreign bidders / individuals who wish to submit bids.

13.1.4 It is a requirement that bidders grant a written confirmation when submitting this bid that SARS may on an ongoing basis during the tenure of the contract disclose the bidder's tax compliance status and by submitting this bid such confirmation is deemed to have been granted.

13.1.5 Bidders are required to be registered on the Central Supplier Database and the National Treasury shall verify the bidder's tax compliance status through the Central Supplier Database.

13.1.6 Where Consortia / Joint Ventures / Sub-contractors are involved, each party must be registered on the Central Supplier Database and their tax compliance status will be verified through the Central Supplier Database.

13.2 Procurement Legislation

The International Trade Administration Commission of South Africa has a detailed evaluation methodology premised on Treasury Regulation 16A3 promulgated under Section 76 of the Public Finance Management Act, 1999 (Act, No. 1 of 1999), the Preferential Procurement Policy Framework Act 2000 (Act, No.5 of 2000) and the Broad-Based Black Economic Empowerment Act, 2003 (Act, No. 53 of 2003).

13.3 Technical Legislation and/or Standards

Bidder(s) should be cognizant of the legislation and/or standards specifically applicable to the services.

14. Contract Documents

14.1 This Request for proposal and all its Technical and Administrative Annexures, together with the accepted Bidding Documents, duly completed and submitted by the successful bidder, shall form part of the Contract Documentation, according to which this project shall be undertaken, managed and completed.

14.2 The contract shall commence upon receipt of the letter of appointment and the purchase order from ITAC by the successful bidder.

15. Evaluation of proposal received

The International Trade Administration Commission of South Africa has set minimum standards (stages) that a bidder needs to meet to be evaluated and selected as a successful bidder. The minimum standards consist of the following:

Initial Screening process (Stage 1)	**Technical Evaluation Criteria (Stage 2)**	**Price and Specific goals evaluation (Stage 3)**
Bidders must complete, sign and submit all Standard Bidding Documents (SBD), as outlined in paragraph 12. Bidders must also be Tax Compliant as per requirements of paragraph 13. **NB: Bidders will be disqualified if SBD 4 form is not submitted, not fully completed and signed. Bidders will also be disqualified if they are not Tax Compliant.**	Bids will be evaluated on compliance with each service category they bid for as per the evaluation criteria for functionality. Bidder(s) will be required to achieve a minimum of 70 points out of 100 points. Only bidders that are considered responsive in terms of Stage 1 (initial screening) and Stage 2 (technical evaluation criteria) will proceed to Stage 3 for Price and Specific Goals evaluation.	The 80/20 preference point system will be used to evaluate bids in Stage 3. Bidder(s) will be evaluated out of 100 points and Stage 3 will only apply to bidder(s) who have met and exceeded the minimum threshold of 70 points. **NB: A bidder that obtains a higher score in terms of price and specific goals will be ranked higher based on the outcome of each category. A rotation system will be applicable once the panel has been finalised and during utilisation.**

ALLOCATION OF WORK

The panel shall be utilised based on ITAC's needs and in accordance with the utilisation guide and principles' below:

- Two service providers will be appointed per category and work will be rotated between the two service providers in each category.
- A bidder that obtains a higher score in terms of price and specific goals will be ranked higher based on the outcome of each category.
- Appointment onto the panel will not guarantee any future work.
- ITAC will utilise the Panel in a manner which promotes the elements of transparency, fairness and equal opportunity in the utilisation and management of the Panel.
- Successful bidders will be informed of their ranking on the panel.
- The service provider appointed onto the panel shall adhere to agreed services standards, including timely response to service requests and any other related correspondence.
- Service requests may only cover services and work falling within the scope of work associated with the agreement which may not be amended for the duration of the contract.
- Service requests may not be issued after the expiry of the term of the panel agreement.

15.1 ITAC reserves the right not to accept the lowest bid, as the elements listed in the evaluation matrix will play a major role, when evaluating bids. Additionally, ITAC is not bound to select any of the bidders or individuals submitting a proposal.

15.2 Prospective bidders are required to complete the SBD 6.1 form to qualify for specific goals as alluded under the evaluation criteria. The CSD report attached or printed by ITAC should also indicate same specific goals claimed as the points indicated on CSD would take precedent.

15.3 Prospective proposals will be evaluated in accordance with the 80/20 preference point system, as contemplated in the Preferential Procurement Policy Framework Act (Act 5 of 2000). Bidders who obtain 70 out of 100 points in stage 2 (technical evaluation) will be added to the Panel, considering the outcome of the Price and Specific Goals evaluation and ranking. Stage 3 (Price and specific goals) will be based on the 80/20 preference points system wherein 80 points for price and 20 points for specific goals.

In respect to the evaluation matrix, prospective bidders will be rated from 1 to 5 in that: 1 = very poor, 2 = poor, 3 = average, 4 = good, 5 = very good.

15.4 To ensure meaningful participation and effective comparison, bidders are requested to furnish detailed information to substantiate compliance with the evaluation criteria.

Stage 2 (Criteria for Technical Evaluation)

Evaluation Criteria	**Weight**	**Scoring**
Project delivery experience **All bidders must demonstrate the minimum required years of experience in the planning, designing implementation, support and maintenance of the various ICT service delivery areas.** Bidders must include 3 relevant reference letters from clients that they have successfully provided the services according to the Terms of Reference. The reference letters must be on company letterheads and must include the type of project, contract amount, contract dates and contact details for ease of reference. No appointment letters from clients will be accepted as reference letters. The references must not be older than 10 years.	20	5 letters = 5 4 letters = 4 3 letters = 3 2 letters = 2 1 letter = 1
Experience of the Technical Team **Certified copies (not older than 3 months) of all qualifications, relevant certificates, and comprehensive and updated curricula vitae is required)**	30	

Project leader Detailed curriculum vitae with a total of 5 years' expertise on similar projects. **Technical lead** Detailed curriculum vitae with a total of 5 years' expertise on similar projects **Junior support expert** Detailed curriculum vitae with a total of 5 years' expertise on similar projects		5 = >10 or more years' experience 4 = 7-8 years' experience 3 = 5-6 years' experience in related area 2 = 3-4 years' experience in related area 1 = 1-2 years' experience in related area 5 = >10 or more years' experience 4 = 7-8 years' experience 3 = 5-6 years' experience in related area 2 = 3-4 years' experience in related area 1 = 1-2 years' experience in related area 5 = >10 or more years' experience 4 = 7-8 years' experience 3 = 5-6 years' experience in related area 2 = 3-4 years' experience in related area 1 = 1-2 years' experience in related area
Project Methodology and Service Level Agreement (SLA) management **Bidder to explain the methodology of delivering services including proposed SLAs metrics for managing the delivery**	30	5 = Detailed Proposal including all the requirements / deliverables including roles and responsibilities, terms and conditions and applicable SLA parameters. 4 = Proposal including some of the deliverables with roles and responsibilities, terms and

of services in terms of timelines, turn-around times, roles and responsibilities, terms and conditions and other applicable SLA parameters. **Proposed sample SLAs must form part of this plan. The sample SLA must include all the standard metrics for managing the delivery of services in terms of timelines, turn-around times, roles and responsibilities, terms and conditions and other applicable SLA requirements.**		conditions and applicable SLA parameters. 3 = Proposal including some of the deliverables excluding roles and responsibilities, terms and condition and applicable SLA parameters. 2 = Proposal excluding majority of the requirements mentioned under scope of service. 1 = No project methodology and service level agreement metrics included.
OEM Certification **Bidders must be Certified OEM Solution Partners (Alternatively, service providers may partner with another organisation with OEM certification) with Vendors who provide the solution/equipment, provide a valid accreditation**	20	**Valid Titanium = 5** **Valid Platinum = 4** **Valid Gold= 3** **Not Valid = 0**

NB: Bidders who obtain 70 out of 100 points in Stage 2 (Technical Evaluation) will qualify for the Stage 3 (Price and specific goals) evaluation wherein 80/20 preference points system will be used as follows: 80 points for price and 20 points for specific goals.

Stage 3 (Criteria for Price and specific goals)

Criteria	**Points**
Comparative Bid Price	80
Specific goals	20
TOTAL	**100**

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

The following formula will be used to calculate the points for price:

Where

Ps = Points scored for comparative price of bid under consideration

Pt = Comparative price of bid under consideration

Pmin = Comparative price of lowest acceptable bid

a. Specific goals (points) allocation

A maximum of 20 points may be allocated to a bidder for attaining their specific goals in accordance with the table below:

The specific goals allocated points in terms of this tender	Number of points allocated (80/20 system) (To be completed by the organ of state)	Number of points claimed (80/20 system) (To be completed by the tenderer)
100% Black Owned	6	
51% - 99% Black Owned	4	
100% Black Women Owned	6	
51% - 99% Black Women Owned	4	
5% Youth Owned	2	
2% Owned by Persons with Disabilities	1	
Business in township, rural or underdeveloped area	2	
Exempt Micro Enterprise (EME)	3	
Qualifying Small Enterprise (QSE)	2	

Specific goals points may be allocated to bidders on submission of the following documentation or evidence:

- A duly completed Preference Point Claim Form: Standard Bidding Document (SBD 6.1); and
- B-BBEE Certificate or Sworn Affidavit (originally certified copies).

The Price and BBBEE points will be consolidated and bidders ranked accordingly.

ITAC will use the information in the duly completed Bidding Documents submitted as well as the required supportive documentation to evaluate each bid against the criteria provided in page 24 to 30.

b. Joint Ventures, Consortiums and Trusts

A trust, consortium or joint venture, will qualify for points for their specific goals as a legal entity, provided that the entity submits their B-BBEE status level certificate or Sworn Affidavit.

A trust, consortium or joint venture will qualify for points for their specific goals points as an unincorporated entity, provided that the entity submits their consolidated B-BBEE scorecard as if they were a group structure and that such a consolidated B-BBEE scorecard is prepared for every separate bid.

Bidders must submit concrete proof of the existence of joint ventures and/or consortium arrangements. **International Trade Administration Commission of South Africa** will accept signed agreements as acceptable proof of the existence of a joint venture and/or consortium arrangement.

The joint venture and/or consortium agreements must clearly set out the roles and responsibilities of the Lead Partner and the joint venture and/or consortium party. The agreement must also clearly identify the Lead Partner, who shall be given the power of attorney to bind the other party/parties in respect of matters pertaining to the joint venture and/or consortium arrangement.

16. Closing Date and time

The closing date and time for the submission of the proposal is 27 February 2026 at 11h00 am.

- **Delivery address**
  The DTIC Campus, Block E first floor 77 Meintjies Street, Sunnyside Pretoria 0002

17. Proposal Submission / Responses

Bidders will be required to use the two-envelope system, whereby the technical proposal (stage 2) and pricing and specific goals (stage 3) are placed in two separate envelopes and clearly marked:

TECHNICAL PROPOSAL – Bidders must submit one (1) original and four (4) hard copies of the bid proposal. The original file / envelop must be packaged as follows and clearly marked as "Original"

	Part 1a – Standard Bidding Documents and Administrative Compliance
1	SBD 1-Invitation to Bid
2	SBD 4 – Fully completed and signed Bidder's Disclosure
3	SBD 6.1 – Completed and signed Preference Points Claim Form
4	SBD 7.2 – Completed and signed form
5	General Conditions of Contract – signed
6	Bidder's technical proposal
7	Certified copy (s) of academic or tertiary qualifications
8	Other supporting documents

NB: Bidders will be disqualified if SBD 4 – form is not submitted, not fully completed and signed. Bidders who are not tax compliant on the bid closing date, or who become non-compliant at any time after the closing date, must rectify their tax compliance status within seven (7) working days of being notified to do so. Failure to rectify tax non-compliance within the stipulated period will result in the bidder being disqualified.

FINANCIAL / PRICE PROPOSAL
The attached schedule must be used for Pricing (Annexure C).

NB: The bidder must submit one (1) original financial / price proposal and four (4) hard copies and the envelop must be submitted separately from the technical proposal.

18. Briefing Session : There will be no briefing session. All clarification and information-seeking questions must be submitted via email by 20 February 2026, which will serve as the final cut-off date for enquiries and requests for clarification.

19. Enquiries

Supply Chain Management
Name: Ms. PS Mkhungo
Email: pmkhungo@itac.org.za

Technical Project
Name: Mr. Lehlogonolo Mphago
Email: lmphago@itac.org.za

NB: ITAC RESERVES THE RIGHT TO AMEND THE PROJECT SPECIFICATIONS WITHIN REASONABLE LIMITS.

20. ANNEXURES:

ANNEXURE A: GENERAL CONDITIONS OF CONTRACT
ANNEXURE B: STANDARD BIDDING DOCUMENTS
ANNEXURE C – PRICING SCHEDULE

ANNEXURE C

PRICING SCHEDULE

- Prices must be quoted in South African currency.
- Prices must be inclusive of all delivery costs and taxes. No variation to the accepted quote, will be allowed unless the service provider has obtained prior written approval from ITAC.

1. Cyber Security Services

Cybersecurity Deliverable	Unit	Qty per Year	Year 1 Cost	Year 2 Cost	Year 3 Cost
Baseline Cybersecurity Assessment	Once-off	1			
Quarterly Cyber Governance Report	Per report	4			
Threat Monitoring (EDR/XDR/SOC)	Monthly	12			
Incident Response	Per incident				
Annual Incident Response Simulation	Per test	1			
Bi-annual Tabletop Exercises	Per exercise	2			
Vulnerability Scanning & Reporting	Quarterly	4			
Penetration Test (External + Internal)	Annual	1			
Training & Playbooks	Annual	1			
OEM Licensing (if applicable)	Annual				

2. Server Infrastructure Services

Infrastructure Deliverable	**Unit**	**Qty**	**Year 1**	**Year 2**	**Year 3**
Server Monitoring & Management	Monthly	12			
Patch Management	Monthly	12			
Hyper-V Host Administration	Monthly	12			
VM Provisioning (per VM)	Per VM				
Quarterly Infrastructure Report	Per report	4			
Active Directory Administration	Monthly	12			
High Availability & Load Balancing Support	Monthly	12			
Hardware Lifecycle & Capacity Planning	Annual	1			

3. Cloud Technology Services

Cloud Deliverable	**Unit**	**Qty**	**Yr1**	**Yr2**	**Yr3**
Cloud Readiness Assessment	Once-off	1			
Cloud Governance	Once-off	1			
Cloud Operations	Monthly	12			
Azure Cost Management Reporting	Monthly	12			
Cloud DR Replication Management	Monthly	12			
Annual Cloud Maturity/Health Report	Annual	1			

4. Backup & Disaster Recovery

DR/Backup Deliverable	Unit	Qty	Yr1	Yr2	Yr3
Backup Management	Monthly	12			
Backup Restore Tests	Quarterly	4			
Annual DR Simulation Exercise	Per simulation	1			
Secondary DR Site Maintenance	Monthly	12			
Annual DR Assessment	Annual	1			

5. Network & Network Security

Network Deliverable	Unit	Qty	Yr1	Yr2	Yr3
LAN/WAN Monitoring	Monthly	12			
Firewall Management	Monthly	12			
Network Performance Reporting	Monthly	12			
Network Device Patch Management	Monthly	12			
Annual Network Security Assessment	Annual	1			

Section B: Personnel Pricing

Role	Hourly Rate: Y1	Hourly Rate: Y2	Hourly Rate: Y3	Estimated Hours per Month
Project Lead				10 hours
Technical Lead				20 hours
Junior Support				40 hours

Section C: On-Demand Activities

Activity	Unit Rate
Onsite call-out per hour	
After-hours support (per hour)	
Travel rate per KM	
Professional services (e.g. consulting)	