REQUEST FOR QUOTATION
APPOINTMENT OF A SUITABLY QUALIFIED SERVICE PROVIDER TO DELIVER AN ENTERPRISE CYBERSECURITY MATURITY ASSESSMENT, SECURITY ARCHITECTURE REVIEW, VAPT, CRITICAL ASSET CONFIGURATION REVIEW, IT/OT INTEGRATION TESTING, OT SITE ASSESSMENTS, CYBERSECURITY STRATEGY AND ROADMAP, AND AUTOMATED GRC PLATFORM FOR PRASA.

1. INTRODUCTION

The purpose of this RFQ is to appoint a suitably qualified service provider to deliver an Enterprise Cybersecurity Maturity Assessment, Security Architecture Review, VAPT, Critical Asset Configuration Review, IT/OT Integration Testing, OT Site Assessments, Cybersecurity Strategy and Roadmap, and an automated GRC platform for PRASA.

2. BACKGROUND INFORMATION

The Passenger Rail Agency of South Africa (PRASA) operates critical national rail infrastructure that supports passenger mobility, economic activity, and public safety. As a state-owned entity managing safety-critical rail operations, PRASA is increasingly dependent on interconnected Information Technology (IT) and Operational Technology (OT) systems.
From a cybersecurity perspective, PRASA faces a complex and evolving threat landscape due to:

- **Critical Infrastructure Exposure**: Rail signalling systems, train control systems, telecommunications networks, and station infrastructure are classified as critical infrastructure and are potential targets for cyber disruption.
- **IT/OT Convergence Risks**: Increasing integration between enterprise IT systems and OT environments (e.g., signalling, SCADA, access control systems) creates expanded attack surfaces and risk pathways.
- **Legacy OT Systems**: Many operational systems are long lifecycle, legacy technologies that may lack modern security controls and are difficult to patch or upgrade.

- **Safety and Operational Impact**: Cyber incidents in rail environments can directly impact **passenger safety, service continuity, and operational reliability**.
- **Regulatory and Audit Pressures**: PRASA is required to comply with national legislation (e.g., POPIA, Cybercrimes Act) and demonstrate strong governance in line with audit and public sector accountability requirements.
- **Emerging Cyber Threats**: Increasing global targeting of transport and rail sectors, including ransomware, supply chain attacks, and OT-specific threat actors.

In response to these challenges, PRASA has established a new Chief Information Security Officer (CISO) function to provide dedicated cybersecurity leadership. However, as a newly established capability, the CISO requires structured support to rapidly build, stabilise, and mature the cybersecurity function.

This RFQ therefore seeks to appoint a service provider to support and enable the CISO in establishing a robust, fit-for-purpose cybersecurity capability aligned to the unique risks of rail operations and OT environments.

3. OBJECTIVE OF THE PROPOSED PROJECT

3.1 Programme Objectives

The Cybersecurity Programme commissioned through this RFQ is structured around nine (9) interlinked objectives, each of which is reflected in the scope of work and deliverables.

Ref.	Objective	Definition
O1	**Cyber Maturity Baseline**	Establish a defensible, evidence-based enterprise cybersecurity maturity baseline using NIST CSF 2.0 across the six (6) functions (Govern, Identify, Protect, Detect, Respond, Recover), with explicit mapping to ISO/IEC 27001:2022, ISO/IEC 27002:2022, COBIT 2019, NIST SP 800-53 r5 and applicable South African statutory and regulatory instruments.
O2	**Security Architecture Assessment**	Assess the current-state enterprise security architecture across network, identity, endpoint, data, application, cloud and IT/OT integration domains, applying SABSA and NIST CSF Profile constructs, and produce a target-state reference architecture aligned to a defined Zero Trust maturity trajectory.

O3	**VAPT**	Perform vulnerability assessment and penetration testing across external Internet-facing perimeter, internal corporate network, web applications, mobile applications (iOS, Android), and Application Programming Interfaces (REST, SOAP, GraphQL), using CREST-aligned methodologies and the OWASP Testing Guide (v4.2), OWASP MASVS / MASTG and OWASP API Security Top 10 (2023).
O4	**Critical Asset Configuration Review**	Conduct a configuration security review of critical assets on-premise and in the cloud, benchmarked against CIS Benchmarks (current versions), vendor hardening guides, NIST SP 800-53 / 800-171 / 800-207, and CSA Cloud Controls Matrix (CCM v4).
O5	**IT/OT Secure Integration Test**	Assess and test the secure integration boundary between corporate IT and Operational Technology, applying the Purdue Enterprise Reference Architecture, IEC 62443-3-2 / 3-3, NIST SP 800-82r3, and recognised industry guidance for OT/IT convergence.
O6	**OT Site Cybersecurity Assessment**	Perform an in-depth cybersecurity assessment of three (3) operationally significant sites to be jointly selected with PRASA, applying IEC 62443-2-1 and 62443-3-2 risk-based methodology, non-intrusive passive techniques, physical and procedural security review, and recovery readiness evaluation.
O7	**Strategy and Roadmap**	Translate findings into a board-ready, three (3) year cybersecurity strategy and an eighteen (18) to thirty-six (36) month execution roadmap with sequenced initiatives, indicative capital and operational expenditure, target-state KPIs/KRIs, organisational design implications and compliance traceability.
O8	**CISO Execution Support**	Provide focused advisory support to the newly appointed CISO during the engagement, including executive enablement, governance instruments (policies, standards, charters), board and committee artefacts, and a tactical first-90-days execution plan post-strategy approval

O9	**Permanent GRC Platform Capability**	Implement a permanent, automated GRC platform that converts all assessment outputs (maturity, architecture, configuration, OT, and risk) into continuously monitored compliance and risk records. The platform must deliver real-time dashboards, automated evidence collection, financial risk quantification, and reporting aligned to multiple frameworks (e.g., NIST, ISO 27001, POPIA), including board-ready outputs. PRASA must take full ownership and operation after implementation, supported by knowledge transfer. Simply delivering assessments or strategy documents without a live, ongoing GRC platform does not meet the requirement.

3.2 Expected Outcomes

On successful completion of the engagement, PRASA expects to have realised the following measurable outcomes:

- A quantified enterprise cyber maturity score, by NIST CSF 2.0 function and category, with verifiable evidence trail and clear delta from current state to target state.
- An auditable inventory of vulnerabilities and security exposures across the assessed estate, prioritised on a risk basis with PRASA-contextualised CVSS / DREAD scoring and remediation paths.
- A documented current-state and target-state security architecture, with a clearly defined Zero Trust adoption pathway.
- Defensible configuration baselines for critical on-premise and cloud assets, with measured deviation against industry benchmarks.
- An assessed IT/OT integration boundary with documented control gaps, compensating controls and a tested set of recommendations.
- Three (3) site OT cybersecurity assessment reports, each providing a site-level cyber risk register, prioritised treatment plan and lessons learned applicable to the wider OT estate.
- A board-approved three (3) year cybersecurity strategy with an executable roadmap, financial envelope and quarterly milestone plan.
- A CISO empowered with the artefacts, briefings, governance instruments and ninety (90) day plan required to drive execution from day one of approval.
- Deliver a permanently operational GRC platform fully owned and run by PRASA, with all programme findings embedded as continuously monitored compliance and risk records. By close-out, the platform must provide real-time multi-framework dashboards, automated evidence collection, financial cyber risk quantification, integrated risk registers (including architecture, configuration, and OT), third-party risk management, and POPIA-aligned data privacy management.
- Additionally, PRASA's CISO Office must be fully trained and capable of independently operating the platform, ensuring the programme establishes a lasting, organisation-wide cyber governance capability rather than a one-time assessment.

3.3 Guiding Principles

Bidders are required to demonstrate that their proposed approach aligns to the following guiding principles, which will be assessed during technical evaluation.

- Standards-led: All work products must be traceable to recognised international standards (NIST, ISO/IEC, IEC, CSA) and to South African statutory and regulatory instruments.
- Risk-based: Findings and recommendations must be prioritised by enterprise risk impact, not by raw technical severity alone, with explicit reference to PRASA's business and safety context.
- Evidence-driven: Every finding must be supported by reproducible evidence (screenshots, logs, configurations, scan output, interview notes) retained under chain-of-custody and made available to internal audit and the Auditor-General if required.
- Safety-first: All OT and site-based work must respect rail operational safety primacy. The bidder must comply with PRASA's Safety, Health, Environment and Quality (SHEQ) requirements and operate under formal Permit-to-Work arrangements at all sites.
- Minimum disruption: Active testing must be planned, ring-fenced, communicated and conducted under formal change control. No active or intrusive testing on safety-critical OT systems without explicit written authorisation and OEM sign-off.
- Knowledge transfer: The engagement must measurably uplift the in-house capability of the CISO Office and Group ICT teams, with structured handover, shadowing and documented run-books.
- Defensible execution: All recommendations must be sized, sequenced, costed at indicative level and presented in a form that survives scrutiny by Internal Audit, Group Risk, the Audit & Risk Committee of the Board, and the Auditor-General.

3.4 Out of Scope

The following are explicitly out of scope for this engagement and must not be priced into the bidder's response:

- Implementation, configuration, deployment or operation of any specific security technology, product or platform. Tool implementation may be procured separately by PRASA following completion of the strategy and roadmap. The exclusion does not apply to the GRC automation platform required under Objective O9.
- Operation of an outsourced Security Operations Centre (SOC) or managed detection and response (MDR) service. Operational SOC arrangements are governed by a separate procurement instrument.
- Red team, adversary emulation or covert operations beyond the boundaries set in Section 4 (which are limited to declared, authorised CREST-aligned penetration testing).
- Active or intrusive testing on safety-critical signalling, traction, brake or train protection systems. Assessment of these systems will be limited to passive observation, design review and procedural review.

4. SCOPE OF WORK AND AREAS OF FOCUS

This section defines the work to be performed by the successful bidder. The scope is organised into nine (9) workstreams, each of which is mandatory unless explicitly marked as Optional. Bidders must respond to every workstream with a clear methodology, named team, indicative effort, key inputs required from PRASA, and expected deliverables.

4.1 Workstream 1 – Enterprise Cybersecurity Maturity Assessment

4.1.1 Objective

Establish a quantified, defensible cybersecurity maturity baseline across PRASA's enterprise IT and corporate environment, with explicit applicability to OT through the Govern and Identify functions, using NIST Cybersecurity Framework version 2.0 (CSF 2.0).

4.1.2 In-Scope Coverage

- All six (6) NIST CSF 2.0 Functions: Govern (GV), Identify (ID), Protect (PR), Detect (DE), Respond (RS) and Recover (RC).
- All twenty-three (23) Categories and one hundred and six (106) Subcategories of NIST CSF 2.0.
- All Group ICT-supplied IT services and corporate platforms across PRASA, including but not limited to Active Directory, email, collaboration, ERP, HRIS, FRIS, ticketing back-office, CCTV and access control management platforms, data centre and disaster recovery sites, cloud workloads (where present), end-user computing, perimeter and remote access.
- Group functions in scope for governance and process assessment: Group ICT, Group Risk and Compliance, Group Internal Audit, Group Legal, Group Human Capital, Group Engineering (governance interface only), Group Security (physical security interface), Group Capital Programmes (third-party assurance interface) and the CISO Office.

4.1.3 Required Methodology

The bidder must apply the following methodology, with traceability between each step and the final report:

1. Pre-engagement: gather pre-read materials including organograms, policies, standards, prior audit findings, asset registers, network diagrams, incident logs, prior assessment reports and risk registers, all under NDA.
2. Stakeholder interviews: structured interviews with a defined list of role holders across all in scope functions, using a documented interview pack.
3. Evidence collection: documentary, configuration and operational evidence to support each Subcategory rating, retained under chain-of-custody.
4. Maturity scoring: per-Subcategory scoring on a calibrated 0–5 scale (Non-Existent / Initial / Repeatable / Defined / Managed / Optimised), with rationale and evidence reference for each score.
5. Cross-walk and mapping: explicit mapping of each Subcategory to ISO/IEC 27001:2022 controls, ISO/IEC 27002:2022, NIST SP 800-53 r5, COBIT 2019, the King IV Code on

Corporate Governance, and the National Cybersecurity Policy Framework (NCPF) of the Republic of South Africa.

6. Gap analysis: identification and quantification of gaps between current state and a defined target state aligned to PRASA's risk appetite and the requirements of a Schedule 3B state owned entity operating critical infrastructure.
7. Validation: walk-through of preliminary findings with the CISO and accountable function heads prior to report finalisation.

4.1.4 Specific Deliverables

- Cyber Maturity Assessment Report (Executive Summary, full report, evidence appendices).
- Per-Subcategory scoring workbook with evidence references and rationale.
- Maturity heatmap by Function, Category and Subcategory.
- Compliance traceability matrix (NIST CSF ↔ ISO 27001:2022 ↔ NIST 800-53 ↔ COBIT 2019 ↔ POPIA ↔ NCPF).
- Target-state proposal aligned to PRASA's risk appetite, ready for endorsement by the Risk & ICT Sub-Committee of the Board.
- Board-grade presentation deck (≤25 slides) summarising posture, gaps, peer comparison and recommended priorities.

4.2 Workstream 2 – Security Architecture Assessment

4.2.1 Objective

Conduct an end-to-end review of PRASA's enterprise security architecture, identify design and control gaps, and propose a target-state reference architecture that supports digital transformation, Zero Trust adoption and IT/OT convergence in a controlled manner.

4.2.2 In-Scope Architecture Domains

- Network architecture: corporate LAN/WAN/SD-WAN, data centre fabric, perimeter, DMZ design, segmentation/micro-segmentation, remote access (VPN/ZTNA), guest and Wi-Fi networks, BYOD/MDM enclaves, and connectivity to all known third parties, integrators and partners.
- Identity architecture: Active Directory Forest/domain design, federation (SAML/OIDC), Privileged Access Management, MFA coverage, Conditional Access policy posture, service account hygiene, identity lifecycle and joiner-mover-leaver processes.
- Endpoint architecture: EDR/AV coverage, baseline hardening, patch management, application control, USB/peripheral control, mobile device management for corporate and BYOD.
- Data architecture: classification, labelling, encryption-at-rest and in-transit posture, DLP coverage, data discovery, data residency in cloud, retention and disposal.
- Application security architecture: SDLC, secure coding, SAST/DAST/SCA integration, secrets management, API gateway and management.

- Cloud security architecture: cloud landing zone(s), IAM, network security, encryption, logging, monitoring, CSPM/CWPP coverage, container/Kubernetes posture (where applicable), serverless posture.
- Monitoring and detection architecture: SIEM, log sources, use-case library, detection coverage against MITRE ATT&CK (Enterprise) and MITRE ATT&CK for ICS, threat intelligence integration, SOAR posture.
- IT/OT boundary architecture (interface to Workstream 5 and 6): DMZ, jump hosts, unidirectional gateways, asset visibility platforms (Claroty, Nozomi Networks, Dragos, Tenable.ot, Forescout or equivalent), OT-specific monitoring.
- Security operating model: SOC architecture, escalation, integration with NCC-CSIRT and sectoral peers.

4.2.3 Required Frameworks and Reference Models

The bidder must produce its target-state architecture using a combination of:

- SABSA Enterprise Security Architecture Framework (Strategic Architecture and Conceptual Architecture layers as minimum).
- NIST CSF 2.0 Profiles (Current Profile, Target Profile).
- NIST SP 800-207 Zero Trust Architecture, supplemented by CISA Zero Trust Maturity Model v2.
- Purdue Enterprise Reference Architecture (for IT/OT boundary).
- CSA Enterprise Architecture Reference Model and CCM v4 (for cloud).
- ISO/IEC 27033 (network security).

4.2.4 Specific Deliverables

- Current-State Security Architecture Report with diagrams (logical, physical, control).
- Target-State Security Reference Architecture with diagrams and design principles.
- Zero Trust Maturity Assessment and Adoption Pathway aligned to CISA ZTMM v2.
- Architecture Risk Register with prioritised remediation options.
- Decision-grade architecture pattern catalogue for re-use across digital programmes.

4.3 Workstream 3 – Vulnerability Assessment and Penetration Testing (VAPT)

4.3.1 Objective

Identify, validate and contextualise security vulnerabilities and exploitable weaknesses across PRASA's external, internal, application, mobile and API estate. All testing must be conducted under formal Rules of Engagement (RoE) signed prior to test commencement, with PRASA-supplied points of contact for emergency stop and escalation.

4.3.2 Methodology Standards

Bidders must conduct testing in accordance with the following recognised methodologies as applicable:

- CREST Penetration Testing Guide and CREST OWASP Verification Standard (CREST OVS).
- OWASP Web Security Testing Guide (WSTG) version 4.2 or later.

- OWASP Mobile Application Security Verification Standard (MASVS) and Mobile Application Security Testing Guide (MASTG).
- OWASP API Security Top 10 (2023) and OWASP API Security Verification Standard (ASVS L2 minimum).
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.
- PTES (Penetration Testing Execution Standard).
- MITRE ATT&CK (Enterprise) for adversary technique mapping.

4.3.3 VAPT Components

4.3.3.1 External (Internet-Facing) Penetration Testing

- OSINT and reconnaissance against all PRASA-owned Internet-exposed assets, domains, cloud tenants and identity providers.
- Network and service enumeration, vulnerability identification and validation, manual exploitation of validated weaknesses (within agreed RoE).
- Email security (SPF, DKIM, DMARC, BIMI), DNS security, certificate posture, exposed administrative interfaces, and credential exposure on the surface, deep and dark web.
- Cloud surface review: cloud provider IAM, exposed buckets/blobs/containers, exposed APIs and serverless endpoints.

4.3.3.2 Internal Network Penetration Testing

- Authenticated and unauthenticated testing from a defined corporate jump-off point.
- Active Directory security assessment including BloodHound-aligned attack-path analysis, Kerberos misconfigurations, ACL abuse, GPP/GPO weaknesses, ADCS/PKI hygiene, and tier-zero asset exposure.
- Lateral movement, privilege escalation and persistence simulation under controlled conditions, mapped to MITRE ATT&CK Enterprise tactics and techniques.
- Segmentation validation between corporate zones, guest networks, DMZ, OT DMZ and Cloud landing zones.

4.3.3.3 Web Application Penetration Testing

- All in-scope production and pre-production web applications, including authenticated and unauthenticated user roles, administrative roles, B2B and B2C interfaces, ticketing front-ends, passenger portals and corporate web platforms.
- OWASP Top 10 (2021) and OWASP ASVS L2 verification.
- Manual logic flaw testing in addition to automated scanning. Pure scanner output will not be accepted as a deliverable.

4.3.3.4 Mobile Application Penetration Testing

- All PRASA-issued or PRASA-branded mobile applications on iOS and Android.
- Static analysis (reverse engineering, secrets exposure, insecure storage, weak cryptography).
    - Dynamic analysis (transport security, certificate pinning bypass, runtime instrumentation, anti-tamper controls, IPC abuse).

- Backend service interaction (linked to API testing below).
- OWASP MASVS L2 verification.

4.3.3.5 API Penetration Testing

- All in-scope REST, SOAP and GraphQL APIs supporting PRASA platforms, including third-party integrations.
- OWASP API Security Top 10 (2023) coverage: BOLA, BFLA, broken authentication, mass assignment, server-side request forgery, improper inventory management.
- Rate limiting and abuse case testing, business logic, schema/contract enforcement.
- Authentication and authorisation deep-dive (OAuth 2.x, OIDC, JWT, API keys, mutual TLS).

4.3.3.6 Optional: Breach and Attack Simulation

As an optional (separately priced) component, the bidder may include the deployment of a Breach and Attack Simulation (BAS) capability for a bounded period (maximum eight (8) weeks) to validate detection coverage and provide a benchmark of preventive and detective control effectiveness. PRASA will retain sole discretion on activation.

4.3.4 Reporting Requirements

- Each VAPT component must produce: an Executive Summary, a Technical Findings Report with PoC evidence (redacted screenshots, request/response, command output, network captures where appropriate), a Remediation Action Plan with sequenced steps and verification criteria, and a Retest Report following remediation.
- All findings must include: CVSS v3.1 base and environmental score, CWE reference, MITRE ATT&CK technique mapping where applicable, OWASP category, PRASA-contextualised risk rating, affected asset(s), root cause, recommended fix and verification approach.

4.4 Workstream 4 – Critical Asset Configuration Review

4.4.1 Objective

Conduct a configuration security review of PRASA's critical on-premise and cloud assets, benchmarked against recognised industry hardening baselines, with quantified deviation, prioritised remediation, and ready-to-execute configuration baselines for sustained enforcement.

4.4.2 In-Scope Assets (Indicative)

The final asset list will be agreed with PRASA in the inception phase. Indicative scope:

On-Premise Assets

- Windows Server estate (Domain Controllers, member servers, application and database servers, file servers).
  - Linux/UNIX server estate (RHEL, Ubuntu, SUSE).
  - Hypervisors (VMware vSphere, Microsoft Hyper-V, FusionCompute).
  - Database platforms (Microsoft SQL Server, Oracle, PostgreSQL, MySQL).
- Network devices (Huawei, Cisco, etc.)
- Wireless infrastructure controllers and access points.

- Backup and recovery platforms (e.g. Commvault).
- Critical middleware, identity stores and PKI (Active Directory Certificate Services, dedicated PKI appliances).

Cloud Assets

- Public cloud tenants in scope (AWS, Microsoft Azure, Google Cloud Platform, Huawei, etc.).
- Cloud foundational services: IAM, organisations/tenants, networking (VPC/VNet, peering, transit), Key Management Services, logging and monitoring services.
- Cloud-native workloads: compute, storage, database-as-a-service, container platforms (EKS/AKS/GKE), serverless.
- Software-as-a-Service tenants critical to PRASA (e.g., Microsoft 365, Google Workspace if applicable), and any business-critical SaaS platforms.

4.4.3 Benchmarks and Standards

- CIS Benchmarks – current versions for each in-scope platform.
- Vendor hardening guides (Microsoft Security Compliance Toolkit, Red Hat STIG-aligned guides, VMware Security Configuration Guide, network vendor hardening guides).
- DISA STIGs (where applicable as a secondary reference).
- NIST SP 800-53 r5, 800-171 r3, 800-207, 800-210 (cloud).
- CSA Cloud Controls Matrix v4.
- ISO/IEC 27002:2022, where applicable.

4.4.4 Required Outputs

- Per-asset configuration deviation report with severity and remediation guidance.
- PRASA-tailored hardening baselines / Group Policy and configuration packages ready for adoption.
- Configuration drift detection recommendations and pilot plan.
- Cloud security posture assessment with cloud-by-cloud findings and ready-to-deploy remediations.

4.5 Workstream 5 – IT/OT Secure Integration Test

4.5.1 Objective

Assess and test the security of the integration boundary between PRASA's corporate Information Technology environment and its Operational Technology environment, with the objective of validating that the boundary is correctly designed, correctly implemented, and provides defensible protection against IT-originated and OT-originated threats.

4.5.2 In-Scope Integration Points (Indicative)

- Industrial DMZ design, including IT-OT firewalls, proxies, jump hosts, file transfer gateways, historian replication and unidirectional gateways where present.
- Identity and access management bridge between IT (Active Directory, federation) and OT (local accounts, engineering workstations, HMI accounts).

- Remote vendor access pathways (OEM/integrator remote access for signalling, traction, station automation, CCTV, ticketing OT, depot automation).
- Telemetry, monitoring and asset-visibility flows from OT into SOC/SIEM platforms.
- Patch, antivirus, configuration management and backup pathways crossing the IT-OT boundary.
- Engineering workstation usage policies and operational practice (USB hygiene, transient devices, vendor laptops).

4.5.3 Required Frameworks

- Purdue Enterprise Reference Architecture (PERA), Levels 0–5.
- IEC 62443-3-2 (Security risk assessment for system design).
- IEC 62443-3-3 (System security requirements and security levels).
- NIST SP 800-82 Revision 3 (Guide to Operational Technology Security).
- ISA/IEC 62443-2-4 (Security program requirements for IACS service providers) – for assessing integrator and OEM service arrangements.
- CISA Cross-Sector Cybersecurity Performance Goals (CPGs) – OT extensions.

4.5.4 Approach Constraints

SAFETY-CRITICAL CONSTRAINT

No active or intrusive testing is permitted against safety-critical OT systems including, without limitation, signalling, train protection, traction, brake control, level-crossing control, points and trackside equipment, without explicit prior written authorisation from the Group Chief Operating Officer, the responsible Engineering Executive, the responsible OEM, and the CISO. Assessment of these systems will be limited to passive observation, design and configuration review, and procedural review under Permit-to-Work conditions.

4.5.5 Deliverables

- IT/OT Boundary Current-State Assessment Report.
- Test results from authorised IT-OT integration tests (network segmentation validation, identity bridge testing, vendor access pathway review).
- Recommendations for IT/OT secure integration target-state, aligned to Workstream 2 architecture outputs.
- Vendor / integrator remote access policy and standard recommendation.

4.6 Workstream 6 – OT Cybersecurity Assessment (3 Selected Sites)

4.6.1 Objective

Conduct an in-depth cybersecurity assessment of three (3) operationally significant PRASA sites, jointly selected with the bidder following inception. The objective is to establish a site-level cyber risk picture, identify safety-relevant exposures, validate the resilience of critical operational

processes, and produce site-specific treatment plans that can be replicated across the wider OT estate.

4.6.2 Site Selection Criteria

Sites will be selected jointly with PRASA based on operational criticality, representative diversity (e.g., one signalling/control facility, one depot/maintenance facility, one major station or interchange), and feasibility of safe assessment access. Final selection requires approval by the *CISO* and the Programme Sponsor.

4.6.3 Required Methodology

- Site-level threat, vulnerability and risk assessment aligned to IEC 62443-3-2 and IEC 62443-2-1.
- Asset and zone-and-conduit inventory development or validation (Levels 0–3).
- Network architecture review (logical and physical), including review of as-built diagrams against actual deployment.
- Passive network traffic analysis using OEM-approved, agreed tooling (Claroty Continuous Threat Detection, Nozomi Guardian, Dragos Platform, Tenable.ot, Forescout eye Inspect or equivalent), conducted in span/mirror configuration only.
- Configuration review of selected OT components (HMIs, engineering workstations, historians, OT-side jump hosts, OT firewalls) under PRASA Permit-to-Work.
- Physical and environmental security review of OT cabinets, control rooms, comms rooms and trackside enclosures within the assessed sites.
- Review of operational procedures: change management, vendor access, USB and removable media, incident response, backup and recovery.
- Safety and cyber-physical impact evaluation, with explicit attention to the interaction between cyber events and the rail Safety Management System.

4.6.4 Deliverables Per Site

- Site-Level OT Cybersecurity Assessment Report.
- Site-level asset and zone/conduit register.
- Site-level risk register and treatment plan.
- Photographic and diagrammatic evidence appendix.
- Site-level executive briefing pack (≤15 slides) for Operations leadership.

4.6.5 Cross-Site Synthesis

- Cross-Site OT Cybersecurity Synthesis Report with patterns, root causes and group-level recommendations.
- OT cybersecurity uplift recommendations applicable to the wider PRASA OT estate.

4.7 Workstream 7 – Cybersecurity Strategy and Execution Roadmap

4.7.1 Objective

Translate the findings of Workstreams 1 through 6 into a coherent, board-ready cybersecurity strategy and a defensible execution roadmap with sequenced initiatives, indicative investment requirements, target-state KPIs and KRIs, organisational design implications and compliance traceability.

4.7.2 Strategy Components

- Cybersecurity Vision, Mission and Strategic Objectives, aligned to PRASA's Corporate Plan and the National Cybersecurity Policy Framework.
- Strategic posture statement (cyber risk appetite, target-state maturity).
- Defined strategic themes (e.g., Govern & Risk, Identity-First Security, Resilient Operations, OT Security, Secure-by-Design, Talent & Culture, Third-Party & Supply Chain, Compliance & Assurance).
- Strategic principles to guide cyber investment and operating decisions over the planning horizon.
- Defined target-state operating model and CISO function design.
- KPI / KRI framework with proposed targets and measurement cadence.
- Compliance traceability against POPIA, NCPF, the Cybercrimes Act (Act No. 19 of 2020), King IV, ISO/IEC 27001:2022, NIST CSF 2.0 and Treasury Instructions.

4.7.3 Roadmap Components

- Initiative portfolio: a complete catalogue of all initiatives required to move PRASA from current-state to target-state maturity, each with objective, scope, dependencies, success criteria, indicative effort and indicative cost.
- Roadmap visualisation covering an 18-, 24- and 36-month horizon, with quarterly milestones.
- Sequencing and dependency mapping, including critical-path identification.
- Indicative investment plan: CapEx and OpEx envelope by year, by initiative cluster, with sensitivity analysis.
- Quick-wins package (initiatives executable within 90 days).
- Year-one execution plan with named owners, deliverables, gates and reporting cadence.

4.7.4 Deliverables

- PRASA Cybersecurity Strategy (full document, 60–100 pages).
- PRASA Cybersecurity Roadmap (workbook + visual artefacts).
- Board / Risk & ICT Sub-Committee presentation pack.
- Investment Case (indicative financial envelope, benefits, risk-adjusted ROI).
- Year-One Execution Plan.
- Compliance Traceability Matrix.

4.8 Workstream 8 – *CISO* Execution Support

4.8.1 Objective

Provide focused advisory support to the newly appointed *CISO* during the engagement, ensuring that the strategy and roadmap are immediately executable and that the *CISO* is equipped with the artefacts, briefings and instruments required to drive the first ninety (90) and one hundred and eighty (180) days post-approval.

4.8.2 Activities

- Weekly working session with the *CISO* and *CISO* Office across the engagement.
- Co-production of foundational governance instruments: Cybersecurity Charter, Cybersecurity Policy, Information Security Policy, Acceptable Use Policy, Privileged Access Policy, OT Cybersecurity Policy, Third-Party Cybersecurity Policy, Incident Response Policy and Plan.
- Co-production of supporting standards and procedures (asset management, vulnerability management, change management security review, joiner-mover-leaver, secure development lifecycle).
- Cybersecurity Steering Committee design, charter, RACI and reporting templates.
- Risk and ICT Sub-Committee / Board pack template and inaugural briefing.
- CISO dashboard prototype (executive cyber metrics).
- Day 1, Day 30, Day 90 and Day 180 CISO Execution Plan.
- Stakeholder engagement plan (Group CEO, Group CFO, Group COO, Group CIO, Group Chief Risk Officer, Group Chief Audit Executive, Group Chief Legal Officer, Group Head: SCM, Group Head: HR, Group Head: Security).

4.8.3 Deliverables

- *CISO* Execution Pack: policy and standard library (drafts), governance instruments, stakeholder briefing materials, KPI dashboard prototype, and 90/180-day execution plan.
- Weekly CISO Office briefing notes.
- Programme close-out briefing for the Group CEO and Board.
- At programme close, the bidder must provide evidence that all CISO execution artefacts, governance instruments, reporting templates and execution actions have been loaded into the Workstream 9 GRC platform as live records where applicable.
- The bidder must support structured knowledge transfer for the CISO Office, with platform-specific operational training delivered under Workstream 9.

4.9 Workstream 9 – Automated Governance, Risk and Compliance Platform

4.9.1 Objective

The bidder must implement a permanent, automated Governance, Risk and Compliance (GRC) platform that converts programme outputs into live cyber governance, risk, compliance, privacy and assurance records. The platform must be configured, populated with programme findings, operational at handover, and capable of being owned and operated by PRASA after implementation.

4.9.2 Minimum Functional Scope

- Multi-framework compliance management aligned to NIST CSF 2.0, ISO/IEC 27001:2022, ISO/IEC 27002:2022, POPIA, Cybercrimes Act, NCPF, King IV, COBIT 2019 and IEC 62443.
- Enterprise cyber risk register, issue tracking and remediation management covering findings from all workstreams.
- Evidence management and control traceability, including attachment of supporting evidence and tracking of evidence status.
- Executive dashboards and board-ready reporting for maturity, compliance, risk exposure, remediation progress, KRIs and KPIs.
- Financial cyber risk quantification using FAIR or an equivalent defensible methodology.
- Third-party risk, privacy, policy, exception, audit and assurance management capability.

4.9.3 Platform Deployment and Configuration Requirements

- The platform must be deployed in a PRASA-approved environment with appropriate access control, encryption, logging, backup and audit capability.
- The bidder must configure PRASA-specific roles, workflows, control libraries, dashboards, risk taxonomies, reports and escalation rules.
- Outputs from Workstreams 1 to 8 must be captured in the platform as live records, including risks, findings, remediation actions and CISO execution items.
- The platform must support role-based access, segregation of duties, audit trails, evidence attachments, reporting and data export.

4.9.4 Knowledge Transfer and Operational Handover

- The bidder must train the CISO Office and at least five (5) nominated ICT staff members to administer, operate and report from the platform.
- Training must include administrator training, user training, reporting guidance, workflow management and practical handover sessions.
- The bidder must provide concise runbooks covering routine platform operations, evidence refresh, risk review, reporting, user access and audit preparation.
- Operational handover and administrator readiness are mandatory for programme closure and final payment.

4.9.5 Deliverables

- GRC Platform Implementation and Configuration Design Document.
- Configured and operational GRC platform with approved frameworks, controls, workflows, dashboards and risk registers activated.
- Live compliance dashboard and cross-workstream risk registers.
- Financial cyber risk quantification model and report.
- Platform administrator guide, user guide, reporting guide and operational runbooks.
- Knowledge transfer pack, including training materials, attendance registers and recorded sessions where applicable.
- Steady-state handover pack confirming PRASA ownership, operating model and closure readiness.

5. SPECIFICATIONS OF THE WORK OR PRODUCTS OR SERVICES REQUIRED

5.1 Mandatory Key Personnel

Bidders must provide the below resources accompanied by CVs and relevant certificates.

Bidders are required to nominate a delivery team in line with the role profiles set out below. Each named individual must have a current curriculum vitae and copies of their relevant certifications attached as part of the bid response. Substitution of named personnel during execution is permitted only with prior written consent of the PRASA Chief Information Security Officer (CISO), and only against an individual of equal or better profile.

Role	Minimum Experience	Mandatory Credentials (or recognised equivalent)	Name of the Proposed Resource	Compliance (Yes / No)
Engagement Director	18 years cyber; 8 years client-facing programme leadership.	CISSP and (CISM or CRISC); experience leading at least one multisite critical-infrastructure cybersecurity programme of comparable scale.		
Lead Consultant – Strategy & Maturity	15 years cyber advisory.	CISSP or CISM; demonstrable lead-author experience on at least three NIST CSF or equivalent maturity assessments; degree in Computer Science, Engineering, Information Systems or equivalent. **The Lead MUST be SSA Vetted.**		

Penetration Testing Lead	12 years offensive security.	CREST CCT App and / or CCT Inf (or OSCE3 / OSCP + OSWE / OSEP); evidence of leading large-scale external, internal, application and API test programmes.		
OT / ICS Cybersecurity Lead	12 years industrial environments; 6 years OT cyber.	GICSP and / or IEC 62443 Cybersecurity Expert; documented field experience on at least two operational OT assessments in rail, energy, oil & gas, utilities or transport.		
Security Architecture Lead	12 years architecture roles.	SABSA Chartered (SCF / SCP) and / or TOGAF; CCSP or hyperscaler Security Specialty; experience with Zero Trust reference architectures (NIST 800-207, CISA ZTMM).		
Cloud Security Lead	10 years cyber; 5 years cloud.	CCSK and / or CCSP; AWS Security Specialty and Microsoft SC-100 (or AZ-500); experience with CIS / CSA CCM cloud configuration reviews.		
GRC and Compliance Lead	12 years GRC and audit.	CISA and (CRISC or ISO 27001 Lead Implementer / Lead Auditor); demonstrated experience aligning programmes to POPIA, King IV and NIST CSF.		

Project Manager	10 years programme delivery.	PMP or PRINCE2 Practitioner; preferably with prior delivery of critical infrastructure cyber programmes; full-time allocation for the duration of the engagement.		

6. DELIVERABLES

The successful bidder will produce the following deliverables. All deliverables are subject to PRASA review and formal acceptance against a documented acceptance criterion. Each deliverable must be issued in editable Microsoft Word and / or Microsoft Excel and / or Microsoft PowerPoint format as appropriate, in addition to a controlled-distribution PDF copy. All deliverables must carry version control, classification marking, and an executive summary.

6.1 Master Deliverables Register

Ref.	Workstream	Deliverable	Format	Phase
D-01	Programme	Inception Report (scope confirmation, RoE, refined plan)	DOCX + PDF	Inception
D-02	Programme	Detailed Project Management Plan (PMP) including risk, comms, quality, change, stakeholder plans	DOCX + PDF	Inception
D-03	Programme	Combined Rules of Engagement (RoE) for all VAPT and IT/OT testing activities	DOCX + PDF	Inception
D-04	WS1	NIST CSF 2.0 Cyber Maturity Assessment Report (Executive + Full)	DOCX + PDF	Assessment
D-05	WS1	Per-Subcategory Scoring Workbook with evidence references	XLSX	Assessment
D-06	WS1	Maturity Heatmap and Visualisation Pack	PPTX + PDF	Assessment
D-07	WS1	Compliance Traceability Matrix (NIST ↔ ISO ↔ NIST 800-53 ↔ COBIT ↔ POPIA ↔ NCPF)	XLSX	Assessment

D-08	WS2	Current-State Security Architecture Report (with diagrams)	DOCX + PDF	Assessment
D-09	WS2	Target-State Security Reference Architecture (with diagrams and patterns)	DOCX + PDF	Strategy
D-10	WS2	Zero Trust Maturity Assessment & Adoption Pathway	DOCX + PDF	Strategy
D-11	WS3	External Penetration Test Report (Executive, Technical, Remediation, Retest)	DOCX + PDF	Testing
D-12	WS3	Internal Penetration Test Report	DOCX + PDF	Testing
D-13	WS3	Web Application Penetration Test Report (per application)	DOCX + PDF	Testing
D-14	WS3	Mobile Application Penetration Test Report (per application, iOS & Android)	DOCX + PDF	Testing
D-15	WS3	API Penetration Test Report (per API surface)	DOCX + PDF	Testing
D-16	WS3	Consolidated VAPT Findings Register with risk scoring and remediation plan	XLSX	Testing
D-17	WS3 (Optional)	Breach and Attack Simulation Baseline Report (if activated)	DOCX + PDF	Testing
D-18	WS4	Critical Asset Configuration Review Report (On-Premise)	DOCX + PDF	Assessment
D-19	WS4	Cloud Security Posture Assessment Report (per cloud)	DOCX + PDF	Assessment
D-20	WS4	Per-Asset Configuration Deviation Workbook	XLSX	Assessment
D-21	WS4	PRASA-Tailored Hardening Baselines / Group Policy Packages	Package + DOCX	Assessment

D-22	WS5	IT/OT Boundary Current-State Assessment Report	DOCX + PDF	Assessment
D-23	WS5	IT/OT Secure Integration Test Report	DOCX + PDF	Testing
D-24	WS5	Vendor / Integrator Remote Access Policy & Standard (recommendation)	DOCX + PDF	Strategy
D-25	WS6	OT Cybersecurity Assessment Report – Site #1	DOCX + PDF	Assessment
D-26	WS6	OT Cybersecurity Assessment Report – Site #2	DOCX + PDF	Assessment
D-27	WS6	OT Cybersecurity Assessment Report – Site #3	DOCX + PDF	Assessment
D-28	WS6	Per-Site Asset & Zone/Conduit Register	XLSX	Assessment
D-29	WS6	Cross-Site OT Cybersecurity Synthesis Report	DOCX + PDF	Strategy
D-30	WS7	PRASA Cybersecurity Strategy (three-year)	DOCX + PDF	Strategy
D-31	WS7	PRASA Cybersecurity Roadmap (workbook + visual)	XLSX + PPTX	Strategy
D-32	WS7	Investment Case (CapEx / OpEx envelope, benefits, risk-adjusted ROI)	XLSX + DOCX	Strategy
D-33	WS7	Year-One Execution Plan with named owners and quarterly milestones	XLSX + DOCX	Strategy
D-34	WS7	Board / Risk & ICT Sub-Committee Presentation Pack	PPTX + PDF	Strategy
D-35	WS8	*CISO* Execution Pack (policies, standards, charters, briefing materials)	DOCX + PDF Library	Throughout
D-36	WS8	CISO Dashboard Prototype (executive cyber metrics)	XLSX / PPTX	Strategy

D-37	WS8	Day 1 / Day 30 / Day 90 / Day 180 CISO Execution Plan	DOCX + PDF	Closure
D-38	Programme	Weekly Programme Status Reports	PPTX + PDF	Throughout
D-39	Programme	Monthly Programme Steering Committee Pack	PPTX + PDF	Throughout
D-40	Programme	Programme Close-Out Report and Lessons Learned	DOCX + PDF	Closure
D-41	Programme	Knowledge Transfer Pack (run-books, templates, training materials)	Mixed	Closure
D-42	Programme	Final Programme Executive Briefing to Group CEO and Board	PPTX + PDF	Closure
D-43	WS9	GRC Platform – Steady-State Handover Package: fully operational, on-prem GRC platform with all workstream outputs embedded as live records; all frameworks activated (NCPF, NIST CSF 2.0, ISO/IEC 27001:2022, IEC 62443, POPIA, Cybercrimes Act, King IV); integrations configured with automated evidence refresh; FAIR-based risk quantification enabled; TPRM, privacy, audit, policy, KPI/KRI, PTaaS, and AI governance modules active. Includes complete run-book documentation.	Platform + DOCX	Closure
D-44	WS9	GRC Platform – Knowledge Transfer and Training Programme: structured training for CISO Office and at least five ICT staff covering all modules, integrations, reporting, evidence management, and workflows; includes instructor-led and recorded sessions. Personnel credentialled on completion. Mandatory for programme closure and final payment.	Training Pack + Recorded Sessions	Closure

D-45	WS9	GRC Platform – Live Compliance Dashboard: real-time multi-framework posture (NIST CSF 2.0, ISO 27001:2022, POPIA, NCPF, IEC 62443) with evidence drill-down, remediation tracking, automated daily evidence updates, alerting, and board-ready reporting— fully operational at handover	Platform	Strategy
D-46	WS9	GRC Platform – Financial Cyber Risk Quantification Report: FAIR (or equivalent) model quantifying cyber risk in financial terms; at least five PRASA-specific scenarios with ALE, PML ranges, and treatment impact for Board decision-making.	DOCX + PDF + Platform	Assessment
D-47	WS9	GRC Platform – Live Cross-Workstream Risk Registers: continuously updated registers covering (a) Architecture risks (MITRE ATT&CK mapped, NIST CSF 2.0 & NCPF aligned), (b) Configuration compliance deviations (CIS, ISO 27001 mapped, with drift detection), and (c) OT compliance (IEC 62443, NIST SP 800-82, NCPF aligned). Accessible enterprise-wide and maintained post engagement.	Platform	Assessment / Strategy

6.2 Deliverable Acceptance Process

Each deliverable will follow a formal acceptance process consisting of

(i) the bidder issues the deliverable in draft,
(ii) PRASA reviews and provides consolidated written feedback within ten (10) business days,
(iii) the bidder issues a revised version addressing all feedback,
(iv) PRASA accepts in writing or escalates to the Cybersecurity Steering Committee.

Failure to achieve formal acceptance within two (2) revision cycles will trigger an Issue under the contract's Issue Management process.

6.3 Intellectual Property and Confidentiality

All deliverables produced under this engagement become the property of PRASA and are subject to the confidentiality provisions of the contract. The bidder retains rights to underlying generic methodologies, tooling and reference frameworks. PRASA shall have a perpetual, royalty-free, irrevocable, non-exclusive licence to use, reproduce, modify and distribute the deliverables internally, to its auditors, regulators and selected third parties under appropriate confidentiality arrangements.

7. PROGRAMME TIMELINE

PRASA requires the main programme delivery to be executed and completed within a maximum elapsed period of six (6) calendar months from the date of contract signature and kick-off, followed by a further six (6) months of handholding, stabilisation and post-implementation support.

7.1 High-Level Timeline

The indicative high-level timeline below covers the initial sixteen (16) week core delivery window. Bidders are required to propose their own detailed week-by-week schedule for the full six (6) month delivery period and the subsequent six (6) month handholding period.

Phase	Title	Duration	Key Activities
P0	**Mobilisation & Inception**	Week 1–2	Team mobilisation; kick-off; security clearance and access provisioning; PMP and RoE finalisation; site selection (WS6); detailed schedule baseline; stakeholder map and engagement plan; tool deployment for assessment evidence repository.
P1	**Discovery & Maturity Assessment**	Week 2–6	WS1 maturity interviews and evidence collection; WS2 architecture discovery; WS4 configuration data collection; WS5 boundary discovery; site planning for WS6. First Steering Committee.
P2	**Active Testing**	Week 5–10	WS3 external, internal, web, mobile, API VAPT; WS5 IT/OT secure integration tests; WS6 OT site assessments. Daily test cadence; weekly findings working groups; immediate notification of any critical findings.

P3	**Analysis & Synthesis**	Week 9–13	Cross-workstream synthesis; target-state architecture finalisation; site-cross synthesis; preliminary strategy and roadmap drafting; CISO Office co-production sessions; alignment workshops.
P4	**Strategy, Roadmap & Closure**	Week 13–16	Strategy and Roadmap finalisation; Investment Case; Year-One Execution Plan; Board / Subcommittee presentation; CISO 90/180-day plan; Knowledge Transfer; programme closeout; final deliverables acceptance.

7.2 Key Milestones

Milestone	Description	Target
M1	Contract signature and programme kick-off	**Week 1**
M2	Inception Report and PMP accepted	**End of Week 2**
M3	Rules of Engagement signed for all VAPT/Integration testing	**End of Week 3**
M4	Maturity assessment evidence collection complete	**End of Week 6**
M5	Active testing complete (WS3, WS5)	**End of Week 10**
M6	OT Site Assessments complete (WS6, 3 sites)	**End of Week 11**
M7	Draft Strategy and Roadmap issued for PRASA review	**End of Week 13**
M8	Final Strategy, Roadmap, Investment Case accepted	**End of Week 15**

M9	Board / Risk & ICT Sub-Committee presentation delivered	**Week 16**
M10	Programme close-out and lessons learned accepted	**Week 16**

7.3 Critical Success Factors for the Timeline

Bidders are expected to be realistic about timeline assumptions and to clearly state the PRASA dependencies required to hold the schedule. PRASA undertakes to make available the following:

- Stakeholder availability for interviews and workshops, scheduled in advance.
- Documentation, evidence and read access to assessment artefacts under NDA.
- Access (logical and physical) for testing within the agreed RoE.
- Designated PRASA Programme Manager and workstream-level counterparts.
- Timely review and feedback on deliverables (10 business-day target).
- Site access and Permit-to-Work for OT site assessments.

8. PROGRAMME GOVERNANCE, APPROACH AND QUALITY

8.1 Governance Structure

The programme will be governed through a three-tier structure designed to provide executive direction, delivery oversight and operational coordination.

8.1.1 Tier 1 – Executive Programme Sponsorship

- Programme Executive Sponsor: Group CEO, PRASA.
- Programme Accountable Executive: Group Chief Information Officer (GCIO), PRASA.
- Reporting cadence: monthly executive review, with ad-hoc convening on Critical findings.

8.1.2 Tier 2 – Cybersecurity Steering Committee

- Chair: Group CIO.
- Members: CISO; Group Chief Risk Officer; Group Chief Audit Executive; Group Chief Operating Officer (or delegate); Group Chief Legal Officer (or delegate); Group Head: SCM; representatives of Engineering, Operations and Capital Programmes; bidder Engagement Partner; bidder Programme Director.
- Reporting cadence: every two (2) weeks during P1-P3, weekly during P4.
- Decision rights: scope changes, exception approvals, risk acceptance, deliverable acceptance escalations.

8.1.3 Tier 3 – Programme Delivery Forum

- Chair: *CISO* / Programme Sponsor.
- Members: PRASA Programme Manager, workstream leads from PRASA and bidder, named bidder workstream consultants.
- Reporting cadence: weekly during the engagement, with workstream-level daily stand-ups during active testing phases.

8.2 RACI Overview

Activity	Group CIO	CISO	PRASA PM	Bidder
Scope confirmation	**A**	**R**	**C**	**R**
Methodology selection and approval	**A**	**R**	**I**	**R**
RoE approval	**A**	**R**	**C**	**R**
Stakeholder access and scheduling	**I**	**C**	**R**	**C**
Conduct of assessments and testing	**I**	**C**	**C**	**R**
Evidence collection and retention	**I**	**C**	**I**	**R**
Deliverable production	**I**	**C**	**C**	**R**
Deliverable review and acceptance	**A**	**R**	**C**	**C**
Risk and Issue management	**A**	**R**	**R**	**R**
Strategy and roadmap endorsement	**A**	**R**	**C**	**R**

Board / Sub-Committee reporting	**A**	**R**	**I**	**C**

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed.

8.3 Quality Management

The bidder must operate a documented quality management approach for the engagement, including:

- A named Quality Assurance Lead (independent of the delivery team) who reviews every external deliverable before release.
- Compliance with the bidder's ISO 9001:2015 quality management system.
- Defined acceptance criteria per deliverable, agreed at inception.
- Internal peer review and sign-off process before any deliverable is issued to PRASA.
- Lessons-learned capture at each phase gate.

8.4 Risk and Issue Management

A Programme Risk Register and Issue Log must be maintained from inception, reviewed at every Steering Committee and reported in every status report. Any Critical risk (impact on safety, service continuity, regulatory exposure or programme viability) must be notified within four (4) hours of identification through the agreed escalation protocol.

8.5 Data Protection and Confidentiality

The bidder must operate the engagement in full compliance with the Protection of Personal Information Act, Act No. 4 of 2013 (POPIA), and equivalent international standards. All personal information processed during the engagement is processed on behalf of PRASA as the Responsible Party, with the bidder acting as an Operator within the meaning of POPIA. The bidder must comply with the data processing addendum, where applicable.

- All evidence and findings repositories must be encrypted at rest (AES-256 or stronger) and in transit (TLS 1.2+ with strong ciphers).
- Access to PRASA data must be restricted to named, vetted personnel.
- All bidder personnel must hold valid criminal record clearance and sign individual NDAs.
- Data residency: PRASA may require certain data classes to remain within the Republic of South Africa. Bidders must declare the geographic locations from which the engagement will be delivered and the locations of any data processing.
- Upon engagement closure, all PRASA data must be securely returned and/or destroyed under a signed certificate of destruction.

8.6 Safety, Health, Environment and Quality (SHEQ) Compliance

All on-site work (Workstream 5 sample testing, Workstream 6 site assessments, any other physical visits) is subject to PRASA's SHEQ regime. The bidder is required to:

- Maintain a documented occupational health and safety management system aligned to ISO 45001:2018, given the field-based and operationally sensitive nature of OT and rail infrastructure work.
- Provide proof of valid Public Liability and Professional Indemnity insurance.
- Provide PPE compliant with the site requirements (high-visibility clothing, safety footwear, eye protection where required, additional PPE as directed).
- Comply with PRASA's Permit-to-Work, Site Induction and Safety Briefing requirements before commencing any work at a PRASA site.
- Comply with the Occupational Health and Safety Act, Act No. 85 of 1993, and the Construction Regulations, where applicable.

8.7 Knowledge Transfer

Knowledge transfer is a contractual requirement and not an optional add-on. The bidder must include in its proposal:

- A structured shadowing programme for the *CISO* Office across the engagement.
- Run-books, templates, and how-to guides for the activities being assessed.
- Two (2) facilitated knowledge-transfer workshops at the conclusion of each phase.
- A capability uplift plan covering the *CISO* Office and Group ICT security function.

9. CONTRACT DURATION

- 12 months
- PRASA requires the main programme delivery to be executed and completed within a maximum elapsed period of six (6) calendar months from the date of contract signature and kick-off, followed by a further six (6) months of handholding, stabilisation and post-implementation support.

10. EVALUATION CRITERIA

Interested bidders for this project shall be evaluated in terms of their administrative responsiveness, substantive responsiveness, technical/functional (capacity testing) evaluation and preference points. The evaluation committee shall use the following Evaluation Criteria depicted in table below for the selection of the preferred bidder that shall render / deliver the required works, goods and / or services.

Evaluation Process	Evaluation Component / Points
Stage 1A - Mandatory Compliance	Substantive responsiveness (mandatory)
Stage 1B - Basic Compliance	Administrative Responsiveness

Stage 2	Technical / Functionality Requirements
Stage 3	Pricing and Specific Goals
Price	80
Specific goals	20
TOTAL	**100**

10.1 STAGE 1 - Mandatory and Basic Compliance Requirements (Substantive and Administrative Responsiveness)

STAGE 1A - Mandatory Compliance Requirements (Substantive Responsiveness)

No.	Description of mandatory requirement and evidence to be submitted	Compliant
a)	Completion and submission of all RFQ documentation, including all declarations and all applicable Standard Bidding Documents (SBDs), duly completed and signed where required.	Yes / No
b)	**ISO/IEC 27001:2022 – Information Security Management System certification.** The bidder, or the relevant partner / consortium member responsible for handling PRASA information, vulnerability data, configuration data, and OT site information, must hold a current ISO/IEC 27001:2022 certification. **Evidence required:** Valid certificate issued by an accredited certification body, clearly showing the legal entity name, standard, certificate number, issue date and expiry date. The certificate must be valid at the bid closing date.	Yes / No
c)	**IEC 62443 / OT cybersecurity capability.** The bidder, or its partner / consortium member responsible for OT / ICS cybersecurity work, must demonstrate firm-level OT cybersecurity capability evidenced through certified personnel or equivalent ISA / IEC 62443 programme capability. **Evidence required:** Valid certificates for nominated OT / ICS cybersecurity personnel. At least one of the following must be submitted: ISA/IEC 62443 Cybersecurity Expert; ISA/IEC 62443 Specialist across relevant domains; GICSP; or another	Yes / No

	recognised OT / ICS cybersecurity certification acceptable to PRASA.	
d)	**Technical proposal and qualified resources.** The bidder must submit a complete technical proposal covering all requirements in **Section 5**, including the nomination of qualified resources, CVs, relevant certifications, and clear mapping of proposed personnel to the required roles.	Yes / No

If a supplier / bidder does not submit the mandatory documents and evidence listed in Stage 1A above, the proposal will be disqualified automatically.

STAGE 1B - Basic Compliance Requirements (Administrative Responsiveness)

If the bidder does not submit the following basic compliance documents, the bid may be disqualified. Where permitted by PRASA, these documents must be made available within the specified period after notification, for example within seven (7) days.

No.	Description of requirement	Compliant
a)	Signed Joint Venture, Consortium Agreement or Partnering Agreement, whichever is applicable.	
b)	Original or certified B-BBEE certificate issued by SANAS. Bidder to include affidavit for QSEs and EMEs. In cases of JVs or consortiums, a combined B-BBEE certificate in the name of the JV/Consortium must be submitted.	
c)	CSD supplier registration number *(should a bidder not be registered on CSD, the bidder will be afforded 14 days after the closing date to register accordingly)*.	
d)	Valid Tax Compliance Status PIN issued by SARS, or equivalent tax compliance confirmation acceptable to PRASA.	
e)	Company registration documents.	
f)	Copies of Directors' ID documents.	

10.2 STAGE 2 - Technical / Functionality Requirements

Qualifying bidders shall be evaluated on technicality / functionality after meeting all compliance requirements outlined above. The minimum threshold for the technical/functionality requirements is 70%. Bidders who score below the minimum requirement shall not be considered for further evaluation in **stage 3.**

ITEM	CRITERIA	WEIGHT
1	Company Experience	40
2	Project Methodology and Approach	30
3	Understanding of Rail/Transport Environment and Risk Context	30
	TOTAL	**100**

Details of the scoring methodology presented above are outlined below:

ITEM	CRITERIA	WEIGHT	SCORES
1	**Company Experience:** The bidder, either individually or collectively with its partners and/or consortium members, must demonstrate experience in a minimum of three (3) comparable cybersecurity assessment engagements completed within the past five (5) years. At least one (1) of these engagements must have included an operational technology (OT) or industrial control system (ICS) component. Verifiable client references, with named client contact, role, contact e-mail address and engagement period must be provided. PRASA reserves the right to contact references directly.	40	**0**: No evidence provided or not comparable **1**: One (1) engagement with limited relevance to scope **2**: Two (2) engagements of moderate relevance (partial alignment to cybersecurity assessment scope) **3**: Three (3) engagements clearly aligned to enterprise cybersecurity assessments (e.g., maturity, VAPT, architecture) **4**: Three (3) highly relevant engagements including at least one with IT/OT or ICS scope, demonstrating application of recognised frameworks (e.g., NIST, ISO 27001, IEC 62443) **5**: Four (4) or more highly relevant, complex, multi-domain engagements (IT, OT, architecture, VAPT), including

ITEM	CRITERIA	WEIGHT	SCORES
			at least one in critical infrastructure (transport, energy, utilities) and demonstrable use of IEC 62443
2	**Project Methodology and Approach:** Bidders must provide a detailed methodology for executing the cybersecurity assessment, including approach, tools, standards (e.g., NIST, ISO 27001, IEC 62443), phases, deliverables, and quality assurance mechanisms. The methodology must clearly demonstrate understanding of both IT and OT/ICS environments.	30	**0**: No methodology provided **1**: Generic methodology with little to no alignment to scope or standards **2**: Basic methodology with limited structure and weak linkage to recognised standards **3**: Adequate methodology aligned to recognised standards (e.g., NIST, ISO), covering core assessment activities **4**: Comprehensive, structured methodology covering all major workstreams (maturity, architecture, VAPT, configuration, IT/OT integration, OT sites), with clear phases, deliverables, and standards alignment (NIST CSF, ISO 27001, IEC 62443) **5**: Highly detailed, integrated methodology demonstrating: • End-to-end traceability (evidence → findings → risk → roadmap) • Explicit alignment to NIST CSF 2.0 and IEC 62443 (3-2, 3-3) • Defined QA, validation, and governance processes • Safety-aware OT approach (non-intrusive testing, permit-to-work) • Clear integration across IT and OT domains
3	**Understanding of Rail/Transport Environment and Risk Context**	30	**0**: No understanding demonstrated **1**: Generic understanding of cybersecurity risks

ITEM	CRITERIA	WEIGHT	SCORES
			2: Limited reference to Rail/Transport or critical infrastructure risks **3**: Adequate understanding of Rail/Transport context (IT/OT convergence, regulatory environment) **4**: Strong understanding of: • Rail/transport sector risks • OT/ICS exposure • Regulatory pressures (POPIA, Cybercrimes Act) **5**: Highly contextualised, insight-driven understanding demonstrating: • IT/OT convergence risks • Safety-critical implications • Legacy OT constraints • Practical, risk-based prioritisation aligned to PRASA
	TOTAL	**100**	

Bidders MUST meet the 70% threshold to proceed to Price and Specific Goals evaluation.

10.3 STAGE 3 – Pricing and Specific goals

The following formula shall be used to allocate scores to the interested bidders: The maximum points for this tender are as follows:

Details	Points
Price	80
Specific Goals	20
Total Points for Price and Specific Goals	100

FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

POINTS AWARDED FOR PRICE

THE 80/20 PREFERENCE POINT SYSTEMS

A maximum of 80 points is allocated for price on the following basis:

80/20

$$Ps = 80 \times [1 - ((Pt - Pmin) / Pmin)]$$

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

POINTS AWARDED FOR SPECIFIC GOALS

In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender.

SPECIFIC GOALS

Note to tenderers: *The tenderer must indicate how points are claimed for each specific goal and must not leave the points claimed column blank.*

The specific goals allocated points in terms of this tender	Returnable	Number of points allocated (80/20 system)	Number of points claimed (80/20 system)
Black Women Owned	Certified copy of ID documents of the owners	5	
Black Youth Owned	Certified copy of ID documents of the owners	5	
Owned by Black People with Disability	Certified copy of ID documents of the owners and	5	

	doctor's note confirming the disability		
Entities with B-BBEE of at least Level 1 or Level 2	B-BBEE certificate / signed affidavit. NB: In case of JV, a consolidated scorecard will be accepted.	5	

ANNEXURE A – PRICING TEMPLATE

Milestones Based Payment Schedule

No.	Milestone	Percentage of Contract Value	Deliverables	Price ZAR (Excl. VAT)
1	**Milestone 1**	+-10%	On completion of Inception (D-01)	
2	**Milestone 2**	+-20%	On acceptance of inception, project management, maturity assessment and architecture assessment deliverables (D-02 to D-10).	
3	**Milestone 3**	+-25%	On acceptance of VAPT consolidated reporting and retest sign-off deliverables (D-11 to D-17).	
4	**Milestone 4**	+-20%	On acceptance of configuration review, IT/OT integration and OT site assessment deliverables (D-18 to D-29).	

5	**Milestone 5**	+-15%	On acceptance of strategy, roadmap, investment case, board pack and CISO execution deliverables (D-30 to D-38).	
6	**Milestone 6**	+-10%	On programme closure, after knowledge transfer, close-out reporting, final acceptance of programme deliverables and confirmed operational handover of Workstream 9 platform deliverables (D-39 to D-47).	
7	**Automated GRC Platform**	Once-off	Automated GRC Platform implementation and handover deliverables (D-43 to D-47).	

ANNEXURE B - List of Abbreviations and Defined Terms

The following abbreviations and defined terms are used throughout this RFQ. Bidders are required to use the same definitions in their response unless otherwise stated.

Abbreviation	Description
BAS	Breach and Attack Simulation
B-BBEE	Broad-Based Black Economic Empowerment
CISO	Chief Information Security Officer
CREST	Council of Registered Ethical Security Testers
CSF	Cybersecurity Framework (NIST CSF 2.0)
CSIRT / CIRT	Cyber Security Incident Response Team
CSP	Cloud Service Provider
DAST / SAST	Dynamic / Static Application Security Testing
DCS	Distributed Control System
GCIO	Group Chief Information Officer
GICT	Group Information and Communication Technology Division (PRASA)
HMI	Human-Machine Interface
ICS	Industrial Control System
IEC 62443	International Electrotechnical Commission – Industrial Communication Networks – Network and System Security

NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology (USA)
OEM	Original Equipment Manufacturer
OWASP	Open Worldwide Application Security Project
POPIA	Protection of Personal Information Act, Act No. 4 of 2013
PPPFA	Preferential Procurement Policy Framework Act, Act No. 5 of 2000 (Regulations 2022)
PRASA	Passenger Rail Agency of South Africa (SOC) Limited
RFQ / RFQ	Request for Proposal / Request for Quotation
SCADA	Supervisory Control and Data Acquisition
SCM	Supply Chain Management
SOC	Security Operations Centre
SOC 2	AICPA Service Organization Controls 2 (Type I and Type II)
VAPT	Vulnerability Assessment and Penetration Testing
ZTNA	Zero Trust Network Access