Description of Request	Eskom Employee Voice: appointment of a service provider for the provision, implementation, configuration, support and maintenance of a secure Employee Voice Platform on a five-year subscription for approximately 43,600 employees.

1. High level background

Eskom implemented its first Employee Engagement Survey approximately twelve years ago using internal Human Capital resources and existing platforms. The survey later evolved into the Human Capital Organisational Effectiveness (HCOE) survey, integrating organisational change, culture and employee value proposition measures. The HCOE survey ran from FY2018/19 to FY2023/24 and was placed on hold during FY2024/25.

The previous approach relied on Eskom SharePoint and manual processes. Persistent low response rates, concerns regarding confidentiality and anonymity, outdated diagnostic data, limited real-time analytics and constrained internal IT capacity reduced the usefulness of the survey for timely, evidence-based decision-making.

The last HCOE survey achieved a response rate of 36.5%. Eskom now requires an external, digitally advanced Employee Voice Platform capable of supporting enterprise-wide continuous listening, local and international benchmarking, advanced analytics, action planning and a targeted response aligned with industry norms.

Eskom invites proposals from suitably qualified and experienced service providers to provide, implement, configure, support and maintain a secure, anonymous, inclusive, accessible and scalable Employee Voice Platform on a five-year subscription. The initiative supports Eskom's culture transformation and high-performing ethical organisation agenda by giving employees an effective voice and enabling leaders to act on reliable people and culture insights.

2. Scope of work/Business requirements

Eskom requires an end-to-end Employee Voice Platform and associated professional services for approximately 43,600 employees across Eskom Group, divisions, subsidiaries, organisational units, business units, departments and sections. The contract shall include the software subscription, implementation, configuration, survey methodology, benchmarking, rollout support, analytics, reporting, action planning, change management, training, knowledge transfer, support, maintenance and continuous improvement services for five years.

The bidder shall propose a complete, formally released and supported solution and shall provide a detailed implementation approach, project schedule, resource plan, technical architecture, security response, service model, assumptions, dependencies, exclusions and cost decomposition aligned with the pricing schedule. The solution must support enterprise-wide engagement surveys, culture diagnostics, pulse surveys, targeted

listening and follow-up surveys. Shortlisted bidders may be requested to demonstrate the proposed platform against Eskom use cases and the mandatory requirements in this scope.

The platform must be cloud-hosted. The bidder shall provide the hosting architecture and sizing for production and non-production environments, including availability, resilience, backup, disaster recovery, capacity, performance, data residency, security controls and scalability. Cloud hosting locations, cross-border processing and disaster recovery locations are subject to Eskom Enterprise Architecture, Information Security, Data Governance and POPIA approval. South African and/or European Union hosting is preferred where feasible.

The bidder shall provide a five-year product and technology roadmap covering platform support, planned releases, security updates, AI and analytics capabilities, integration options, accessibility improvements, end-of-support considerations and migration or exit arrangements. Material technology or hosting changes during the contract require prior notification and Eskom approval where applicable.

Project Volumes and Baseline Information

The solution shall accommodate the full eligible workforce and the management and Human Capital user groups that will use dashboards, analytics and action-planning capabilities. Volumes are indicative and may change during the contract. The bidder remains responsible for sizing the platform to meet concurrency, performance, storage and response-time requirements.

Category	Indicative volume
Employees, including FTC	+/- 43,600
Line managers, included in employee total	+/- 3,842
HR Business Partners, included in employee total	+/- 338

Table 1: Project Volumes

The scope shall include:

Deliverable	Description
Functional **Platform Functionality**	• Support engagement, culture diagnostic, pulse, targeted listening and follow-up surveys; explain configuration and management, standard versus configured/customised capabilities, dependencies and limitations. • Enable authorised administrators to configure survey cycles, dates, populations, segments, questions, communications and participation rules; explain approvals, standard/configurable/customised capabilities, dependencies and limitations. • Provide benchmarked engagement, employee experience, high-performance culture and other approved diagnostic frameworks relevant to Eskom; explain dimensions, constructs, scoring, benchmarking, dependencies, limitations and conditions of use. • Allow authorised administrators to add Eskom-specific questions without compromising survey integrity, validity, benchmark comparability, scoring or reporting; explain configuration, review, approval, scoring, reporting, dependencies and limitations. • Provide configurable question libraries, reusable templates, rating scales, open-ended and matrix questions, branching/skip logic and standard response formats; explain administrator configuration, reuse, management, dependencies and limitations. • Provide statistical outputs assessing survey reliability and validity, including approved advanced measures where applicable; explain methods, calculations, data-quality thresholds, interpretation, dependencies and limitations. • Enable secure participation through approved web links, mobile-compatible access and QR codes; explain participant authorisation/validation, anonymity, confidentiality, dependencies, limitations and technical prerequisites. • Support surveys in at least three South African official languages approved during design; explain administrator management of language options, translations, participant selection, version control, dependencies and limitations. • Provide accessibility for Persons Living with Disabilities (PLWD), including assistive-technology compatibility; explain accessibility features, supported technologies, applicable standards/conformance levels, dependencies and limitations.

Deliverable	Description
	• Prevent duplicate, unauthorised and invalid submissions while preserving anonymity and confidentiality; confirm successful submission and record completion status, date and time; explain validation controls and dependencies. • Provide progress indicators, section navigation, mandatory-question validation, save-and-resume, pre-submission review and approved privacy, confidentiality and anonymity notices; explain participant journey, dependencies, configuration and limitations. • Restrict survey viewing and completion to authorised, eligible participants assigned to surveys within approved availability periods; explain eligibility, assignment and access-period controls, dependencies and limitations. • Configure, schedule and distribute targeted invitations, reminders and participation notifications through approved channels, including email and configured mobile channels; explain scheduling, delivery monitoring, dependencies, configuration and limitations. • Preload and associate approved organisational hierarchy and demographic attributes with eligible participants without manual participant entry; explain loading, validation, mapping, updates, protection, dependencies, configuration and limitations. • Provide real-time dashboards and standard reports for authorised executive, management, HR, divisional, regional and functional users, aligned with roles, authority and anonymity thresholds; explain permissions, views, refresh frequency, controls, dependencies, configuration and limitations. • Enable role- and authority-controlled drill-down from enterprise dashboards to permitted organisational and demographic segments, enforcing anonymity thresholds and preventing direct or indirect respondent identification; explain permissions, hierarchies, segmentation, controls, dependencies and limitations. • Provide heat maps, key-driver analysis, trend analysis and priority-focus-area identification for evidence-based decisions; explain methodologies, calculations, data requirements, interpretation, dependencies, configuration and limitations. • Provide clear, role-appropriate visualisations of engagement, employee experience, high-performance measures, response rates and benchmarks aligned with approved reporting definitions; explain formats, configuration, filters, refresh frequency, dependencies and limitations.

Deliverable	Description
	• Compare Eskom results with relevant local/global energy, utility and comparable large-employer benchmarks by index, dimension, authorised segment and approved comparator group; explain methodology, sources, samples, sectors, geography, dataset dates, updates, dependencies, licensing and limitations. • Generate, modify, assign, track and monitor action plans linked to survey results, dimensions, organisational areas and approved priorities, each with an accountable owner; explain workflows, access controls, insight linkages, dependencies, configuration and limitations. • Provide manager guidance, action-plan templates and recommended interventions linked to survey themes, results and priority drivers to support measurable improvements without identifying respondents; explain generation, selection, configuration, maintenance, dependencies and limitations. • Monitor active-survey response rates by approved organisational, demographic, participation and channel dimensions to support targeted interventions while preserving anonymity and confidentiality; explain calculations, refresh frequency, dimensions, filters, controls, dependencies, configuration and limitations. Generate BRS-required executive/manager dashboards and response-rate, benchmark, heat-map, key-driver, action-planning, trend, access/audit and statistical reports; securely export approved outputs to PDF, Excel and PowerPoint under role-based access, anonymity and confidentiality controls; explain processes, dependencies, configuration and limitations.
Functional **Professional Services Functionality**	• Improve survey participation through industry-aligned communications, reminders and targeted interventions; define delivery, governance, triggers, monitoring, dependencies, assumptions and limitations. • Support survey adoption with launch materials, employee and manager guides, FAQs, escalation guidance and reminders; define content approval, deployment, maintenance, dependencies, assumptions and limitations. • Train authorised Eskom stakeholders to manage surveys, reporting, platform administration and action planning; specify audiences, outcomes, delivery, competency assessment, deliverables, dependencies, assumptions and limitations. • Provide accessible, current user, training, administration and support documentation aligned with implemented functionality; define approval, version

Deliverable	Description
	control, updates, distribution, dependencies, assumptions and limitations. Implement, configure, test and deploy the Employee Voice Platform, including surveys, hierarchy and demographic data, user roles, readiness, cutover and post-launch support; define delivery, governance, responsibilities, dependencies, assumptions, risks and limitations.
Solution design and detailed specifications **Functional Specifications and Detailed Design**	Deliver approved solution architecture, configuration design, functional specification, data design, security design, hosting design, operational model, support model and implementation plan, with traceability to Annexure A.
	• Facilitate Eskom reviews and obtain required architecture, cybersecurity, privacy, data-governance and pre-transfer approvals before build and go-live. • Ensure cybersecurity compliance and integration of endpoints. • The Bidder is required to render solution architect services to this project, which includes making sure that all Architecture governance approval is gained before build (Physical Architecture Approval) and again before go-live (Pre-Transfer Approval).
Integration and data enablement **Integration**	Initial implementation requires secure data loading and export. The Service Provider shall ensure data ingestion, transformation, and availability for analytics purposes while maintaining data integrity and security. No direct integration with Eskom systems is required initially. The solution shall nonetheless support future approved integration with identity and access systems, SAP HCM, Power BI, approved repositories, security monitoring and other Human Capital platforms. Ensure: Data consistency, Fault tolerance, Secure data exchange
	• Provide secure interfaces, APIs and documented import/export processes. Future integrations must be subject to Eskom Enterprise Architecture, Information Security, Data Governance, Business approval and change control. • The solution should be able to utilise external REST and SOAP API. The solution should be able to integrate with all other applications as mentioned in the logical design.

Deliverable	Description
	• External interfaces to integrate using Eskom-approved integration platforms and technologies, thus the vendor should be well-skilled to work with the mentioned technologies. • The Integration Centre of Excellence (ICOE) governance process must be followed for all approvals. Kindly reference “SOA Workgroup artefacts”. • The proposed product must have the capability of secure communication when exposing the services via the business services
	The Tenderer must provide technical resources to build and implement all required application-level integration services (Business Services) for the interfaces on the Proposed Product. Please be aware that the Eskom Integration team will do the integration scope for the Middleware activities.
	• Provide application-level integration services (Business Services) that conform to the specific security and Integration standards. • Provide the required detail to the Eskom Integration Team to enable the design of the end-to-end solution and work closely with Eskom’s Integration team. • Provide input and contribute to the Analysis, Design, Message Modelling, Unit testing, SIT testing, UAT testing and Non-Functional testing. • Provide a proposed solution with the capability to support API based integration • Provide a proposed solution with the capability to support API's exposure as services • Have previous experience in the implementation of integration solutions on the proposed product in exposing services for the Middleware communication e.g SOAP, REST Services. • Provide a proposed solution with the capability to support the following list of integration protocols: web services, REST API and SOAP. • Provide the message structure capabilities of the proposed solution. The Solution is to be able to Handle Integration via a Common Information Message (CIM) or if it can only send a proprietary message structure? (Proprietary – Applications own business service message structure)

Deliverable	Description
	• Provide a proposed product with the capability for the Application Business Services to receive an Integration reply with a full-service response (pre-defined message structure) in case the Application is invoking an Integration Web Service. • Provide a proposed product with the capability for the Application Business Services to communicate via One-Way or Two-Way certificate (SSL/TLS) to secure the channel. • Provide a proposed product with the capability for the Application Business Services to support OAuth2 for Web Services, Database or SFTP for Authentication security. • Provide a proposed product with the capability for the Application Business Service to distinguish between Technical and Business error and handle each one in a separate manner. • Provide a proposed product to be able to manage instances where the same record is being published multiple time and not create duplicates
	Initial implementation requires secure data loading and export. The Service Provider shall ensure data ingestion, transformation, and availability for analytics purposes while maintaining data integrity and security. No direct integration with Eskom systems is required initially. The solution shall nonetheless support future approved integration with identity and access systems, SAP HCM, Power BI, approved repositories, security monitoring and other Human Capital platforms. Ensure: Data consistency, Fault tolerance, Secure data exchange
	• Provide secure interfaces, APIs and documented import/export processes. Future integrations must be subject to Eskom Enterprise Architecture, Information Security, Data Governance, Business approval and change control. • The solution should be able to utilise external REST and SOAP API. The solution should be able to integrate with all other applications as mentioned in the logical design.

Deliverable	Description
	• External interfaces to integrate using Eskom-approved integration platforms and technologies, thus the vendor should be well-skilled to work with the mentioned technologies. • The Integration Centre of Excellence (ICOE) governance process must be followed for all approvals. Kindly reference “SOA Workgroup artefacts”. • The proposed product must have the capability of secure communication when exposing the services via the business services
Build, configure and deploy **Build and Deploy**	Configure the platform, benchmarked survey frameworks, Eskom-specific questions, organisational hierarchy, demographic attributes, roles, anonymity thresholds, communication workflows, dashboards, reports, action-planning functions and support processes.
	• Prepare all environments, test configurations, data loads, launch plans, cutover plans, go-live checklists, rollback arrangements, backup and recovery procedures.
	• Obtain all required Eskom governance approvals before production deployment. Provide deployment evidence and an approved go-live readiness pack. • Code to be checked into Eskom’s code repository. • Any development or APIs exposed outside the integration platform will be developed using Eskom software development technology standards, such as .NET technologies, JAVA, and Python.
Testing and assurance **Test**	Manage testing using Eskom-approved processes and tools. Testing shall include configuration and unit testing, system testing, user acceptance testing, security testing, vulnerability assessment, penetration testing, performance testing, accessibility testing, backup/restore testing and disaster-recovery testing, as applicable. The testing team must provide unit test results before resuming the next cycle/level of testing as per the defined entry and exit criteria. A signed-off test closure report is required before a test milestone is completed. The following testing and testing milestones must be completed:

Deliverable	Description
Go-live, hypercare and handover **Stabilise and hand over**	• Support launch, monitor participation and service performance, provide response-rate interventions, stabilise the platform, resolve defects, complete business and support handover, and close implementation after acceptance. • Provide support to stabilise the solution. • Conclude handover to the business. • Conclude handover to support. • Close out the project.
Project and service management **Project Management**	Deliver the approved project charter, detailed schedule, deliverable breakdown structure, RACI, resource plan, risk and issue registers, quality plan, communication plan, change-control log, cash-flow forecast, weekly reports, meeting packs, acceptance certificates and close-out report.
	• List all work packages, milestones, tasks, dependencies, assumptions, exclusions, fixed-cost deliverables and payment milestones. • List all work packages (Milestones) with all tasks and activities to deliver the milestone. • List all work deliverables excluded from this scope of delivery. • Deliverable Breakdown Structure indicating all fixed cost deliverables with the cost of each deliverable and the total cost of all deliverables • Payment schedule forecast and actuals tracking against it. • Weekly progress reports. • Daily or Weekly technical discussion meetings • Delivery Acceptance Certificates with supporting approved test details. • Provide information required by Eskom team members to facilitate governance of the project and its deliverables. • Integrate the current application support teams into the project delivery team.
	• Maintain service performance reporting, incident and problem records, SLA reports, improvement plans,

Deliverable	Description
	release plans and monthly service reviews during the subscription term. • Work Completion Certificates will be completed against approved deliverables, which can then be invoiced. • Projected monthly cash flow. • Update the payment schedule provided every month.
	• The schedule shall reflect mobilisation, design, configure, test, train, deploy, hypercare, operate and exit stages.
Bidder resources and responsibilities **Other Responsibilities**	Provide an organogram and named team with qualifications, experience, certifications, availability and employment status. Dependencies on Eskom and total effort by role must be stated.
	• Minimum roles: Project Director, Survey Methodology Expert, Platform/Technical Lead, Analytics and Insights Lead, Change and Communication Specialist, Fieldwork Coordinator and PMO Coordinator. Replacements require Eskom approval and must be equivalent or better. • Role of person on the proposed team, Description of Education with supporting certificates as proof. • Relevant Experience and Skills. Relevant product certification/s achieved with supporting certificates as proof. • In the case of any personnel exiting the project, the personnel must be replaced with a Change/replacement of personnel equivalent or better.
	• All Eskom-specific deliverables, configurations, reports, action plans, data extracts, documentation, scripts and artefacts shall be provided in maintainable formats. Eskom retains ownership of its data and project-specific intellectual property. • All deliverables shall be provided in a maintainable format for each evaluation (i.e. editable documents, source code and scripts).
	Scope, time and cost changes are subject to formal Eskom change control and delegated approvals.
	• Approved changes shall be documented in governance records and reflected in the baseline, price and delivery schedule. • Depending on the scale of the change, other approvals external to the project may be required.

Deliverable	Description
	• The Project Portfolio Manager will provide guidance in this regard. • Approved changes must be noted in the steering committee minutes.
	• Provide applicable resource rates for authorised changes and optional services.
Security and privacy **Security**	Comply with Eskom information-security requirements, POPIA, approved data classification, anonymity, confidentiality, data sovereignty, incident response, retention, backup, disaster recovery and audit requirements.
	• Provide valid ISO 27001 certification and, for cloud processing of PII or intellectual property, a valid SOC 2 Type II report and bridge letter where required.
	Group Technology Cybersecurity approved authentication, SAML 2.0, OAuth 2.0/2.1, MFA, SSO and future integration with Eskom identity providers.
	• Use RBAC, privileged-access controls, AES-256 encryption at rest, TLS 1.3 or later in transit, SHA-256 or stronger integrity controls, encrypted audit logs, PII masking in non-production and secure backups. • Data must be encrypted at rest.
	• Provide DDoS protection, web application firewall, security monitoring integration, vulnerability management, patch management, e-discovery and cyber-incident notification to Eskom immediately or within 24 hours.
	• Retain and securely dispose of records in line with Eskom requirements. Employee Voice records, reports, action plans, audit logs and knowledge-transfer artefacts must be retained for at least seven years.
Change management and adoption	Provide an integrated change-management strategy, stakeholder plan, communication plan, launch materials, FAQs, manager guides, employee packs, escalation mechanisms and a response-rate improvement strategy.
	Assess organisational impacts and readiness; support leaders and managers; monitor participation; recommend interventions; measure adoption; manage resistance; and align action plans to Eskom transformation outcomes. Change Strategy

Deliverable	Description
	• The bidder is required to create and implement a detailed Change Management Strategy aligned with the project's overarching goals and delivery stages; and • The strategy should explicitly outline the approach to managing changes related to people. Stakeholder Management • Identifying and analysing all stakeholder groups that are affected. • Creating and implementing a plan for engaging stakeholders; and • Continuously managing the expectations and concerns of stakeholders throughout the duration of the project. Communication • Creation of a well-organised communication strategy and plan. • Customised messaging designed for various stakeholder groups. • Concise information regarding project goals, effects, timelines, and anticipated changes; and • Ongoing and uniform communication during all phases of the project. Organisational Impact • Assessment of the effects on the organisation, encompassing roles, responsibilities, access, structures, and job functions; • Mapping of roles and analysis of the impacts on affected users and support functions; and • Align the organisation's structure and access controls with the new solution. Training • Creation and implementation of a detailed training strategy and plan; • Training specific to roles that correspond with the solution future-state solution and business processes; and • Training resources, sessions, and support systems to facilitate successful adoption. Assessment of Impact, Readiness and Adoption • Carrying out assessments of the effects of change; • Evaluating organisational preparedness before significant implementation milestones; and

Deliverable	Description
	• Measuring and reporting on user adoption after the implementation phase. Resistance Management • Identifying potential sources of resistance • Developing and implementing resistance management strategies; and • Actively supporting leadership and management in addressing resistance. The bidder shall assess the business and organisational impacts of the proposed solution and implement appropriate communication, training, readiness, adoption and resistance-management interventions throughout the project lifecycle.

Table 2: Scope

Scope area	Bidder requirement	Evidence
Project approach	Provide the implementation methodology, integrated plan, milestones, dependencies, acceptance points and mobilisation-to-handover schedule.	Plan and schedule
Governance and control	Manage scope, cost, quality, risks, issues, changes, reporting, approvals, deliverable acceptance and close-out.	Governance artefacts
Resources	Provide a qualified project manager and delivery team, with roles, availability, effort, location, Eskom dependencies and approved replacement controls.	Organogram and CVs
Integration and compatibility	Support secure import/export and configurable future integration using Eskom-approved technologies; disclose software, antivirus and licence dependencies.	Architecture and specifications
Security, access and data	Meet Eskom security, POPIA, RBAC, segregation-of-duties, encryption, audit, retention, archiving, backup and data-protection requirements.	Compliance evidence
Resilience and performance	Provide scalable multi-threaded processing, disaster recovery, capacity and performance evidence for 5,000 concurrent users against Eskom targets.	Test and DR results
Testing and quality	Plan and close functional, integration, UAT, security, performance, accessibility, backup and DR testing, including traceability and defect control.	Plans, results and closure reports
Service and support	Meet defect-response and SLA targets; maintain incident, problem, known-issue and improvement records; provide hypercare, handover and exit support.	SLA and support model
Change and training	Deliver stakeholder, communication, adoption and resistance management, plus role-based training, guides, knowledge transfer and effectiveness evidence.	Strategies, materials and records

Table 3: Project Management and Non-Functional Scope for Bidders

High-Level Requirements

The required future state is a single, secure digital Employee Voice ecosystem that supports anonymous survey participation, continuous listening, benchmarked diagnostics, real-time insights, role-based dashboards, action planning and response-rate management. It must support Eskom's diverse and geographically dispersed workforce, including office-based, field-based, non-desk and Persons Living with Disability employees. The solution shall protect respondent identity through approved anonymity thresholds and role-based access while enabling aggregate reporting from Group level to authorised organisational levels.
The bidder shall comply with the detailed functional, reporting, data, user-interface, access, security, archiving, disaster-recovery and service requirements in this document and Annexure A. All mandatory requirements shall be addressed in a traceable compliance matrix.

Security Requirements

The Tenderer must be aware of and comply with the requirements listed below:
1) The Cloud Service Provider (CSP) shall be able to provide a valid Service Organisational Control SOC 2 Type II report when storing and processing Personal Identifiable Information (PII) including Intellectual Property (IP), such attestation report shall be submitted to Eskom for review.

a) Up to once per period of twelve (12) months, the CSP will provide comprehensive summaries of its latest SOC 2 report at no cost upon Eskom's written request

b) if the SOC Report indicate any deficiencies or matter requiring attention, the CSP shall use commercially reasonable efforts to address all such items without any costs to Eskom

c) Subject to Section 1.b, if vendor’s reporting cycle is not aligned with the financial year, and/or the SOC report is older than six (6) months, the CSP shall submit a bridge letter to Eskom at no cost, and such bridging letter shall not cover a period exceeding three (3) months

2) The Tenderer shall have a valid International Organization for Standardization (ISO) 27001 certificate.
3) The system shall be able to integrate with existing Eskom’s Identity Providers (IdP’s) such as Microsoft (MS) Active Directory (AD), Entra Identity (ID) and shall support Security Assertion Markup Language (SAML) 2.0, Open Authorization (OAuth) 2.0 and OAuth 2.1 to enable Multi-Factor Authentication (MFA) and Single Sign-On (SSO).

4) Privileged Access Management (PAM), the system shall be able to onboard privileged accounts onto PAM tools, such as CyberArk but not limited to onboard privileged accounts to securely manage, rotate passwords, monitor, record sessions, enforce access to privileged accounts, auditing and reporting capabilities.

5) The system shall employ Role Base-Access Control (RBAC) mechanism. 6) For all systems that store and process financial information, Personal Information (PI) and Intellectual Property (IP) information, data at rest using minimum Advanced Encryption Standard (AES)-256, data in use and in transit (or in motion) using minimum Transport Layer Security (TLS) 1.3 or later version shall be encrypted.

7) The system shall support Post Quantum Cryptography (PQC) algorithms such as ML-KEM (Module- Lattice-Based Key Encapsulation Mechanism), ML-DSA (Module-Lattice-Based Digital Signature Algorithm) and SLH-DSA (Stateless Hash-Based Digital Signature Algorithm).

8) Data shall be secured at minimum using a Secure Hash Algorithm (SHA)-256 for data integrity, securing transactions, and messages.

9) Audit trails, logs, user administration and user activity logs shall be enabled, encrypted, and securely kept with limited access to administrators.

10) Sensitive information such as PII data in non-production environments shall be masked.

11) Incremental daily back-ups shall be done, encrypted, and securely kept offsite.

12) Real-time data synchronization or data replication to a secondary or Disaster Recovery (DR) site, located in different regions shall be employed.

13) Disaster Recovery Plan (DRP) shall be defined, annually tested, and such DRP test results shall be shared with the Eskom Cybersecurity team.

14) A back-up Restore Plan and Procedure shall be defined, annually tested, and such test results shall be shared with Eskom’s Cyber Security team.

15) Patch Management Process shall be defined. The software updates and patches shall be tested in a non-production environment before being deployed into the production (PROD) environment.

16) The CSP shall comply with applicable privacy and protection of personal information Acts such as General Data Protection Regulation (GDPR) in European Union (EU) and Protection of Personal Information Act (POPIA) in South Africa (SA) where the cloud service is hosted, and the region where the data subjects are physically located and where the data is collected.

17) The CSP shall notify Eskom immediately or within twenty-four (24) hours when any cyber security breach has occurred. Although the General Data Protection Regulation (GDPR) and the South African Cybercrimes Act 19 of 2020 states that the notification shall be sent within seventy-two (72) hours, Eskom shall be notified sooner to allow Eskom to notify the information regulator and take necessary actions to minimize the impact on Eskom.

18) The CSP shall notify Eskom within one (1) month if there are any significant changes to the business, platform and hosting service provider or any change that could have an impact on the security assessment conducted and the auditor's opinion on the System and Organizational Control's (SOC) audit.

19) The database shall be placed behind the perimeter firewall.

20) Distributed Denial of Service (DDoS) protection mechanism shall be employed for all services.

21) Web Application Firewall (WAF) for all internet-facing applications and/or web-based applications shall be employed.

22) The system shall provide e-Discovery capability to identify, collect and produce electronically stored information (ESI) in response to a request for production in a lawsuit or investigation as part of the cloud services offered.

23) The system shall be able to integrate with Security Information and Event Management (SIEM) standard technologies such as Syslog, Windows event logging, Simple Network Management Protocol (SNMP) and Application Programming Interface (API) but not limited to these technologies listed.

A. Additional requirements

A. Existing environment and transition requirements

No historical data migration is required for the initial implementation unless Eskom subsequently approves the use of historical survey results for trend analysis. The bidder shall support secure employee master-data loading, refresh, validation and management for survey administration. Eskom retains ownership of its data and must have continued access to, and an export of, all Eskom data at contract expiry or termination.

B. New functions and features

The solution shall provide continuous listening, enterprise and pulse surveys, benchmarked survey frameworks, AI-enabled insights, statistical validation, executive and manager dashboards, employee high-level summary of the results post the survey, heat maps, key-driver analysis, trend analysis, response-rate monitoring, workflow-based action planning, multilingual capability, accessibility, secure mobile and QR-code participation, and approved data export.

A.1. Project-specific functional requirements

The platform shall enable authorised administrators to configure survey cycles, periods, target populations, organisational segments, questions, communication schedules and participation rules. It shall support question libraries, reusable templates, rating scales, open-text questions, branching logic, save-and-resume where configured, electronic submission, duplicate prevention, completion confirmation, invitations, reminders and participation notifications.

Summary:

A.3.1 Deploy secure, anonymous employee surveys and enforce approved confidentiality and anonymity thresholds across all reports, dashboards, analytics and exports.

A.3.2 Support authorised organisational and demographic segmentation without directly or indirectly identifying respondents.

A.3.3 Provide real-time dashboards, benchmark comparisons, heat maps, driver analysis, trend analysis, response-rate monitoring, notifications and action-plan tracking.

A.3.4 Provide executive, manager, employee high-level summary of the results post the survey, response-rate, benchmark, heat-map, key-driver, action-planning, trend, audit and statistical-analysis reports in approved export formats.

Only authorised and eligible users may access assigned surveys, platform functions, reports or data. Individual employee responses and free-text comments shall not be exposed through dashboards or reports.

B. Employee Voice Platform Functional Scope:

B.1. Employee Voice Platform Functional Scope

The functional scope comprises platform administration, survey design, participation, analytics and dashboards, benchmarking, action planning, response-rate management, security and privacy, data management, reporting, change enablement, knowledge transfer, archiving and retention, disaster recovery, service support and future integration enablement.

B.2. Employee Voice Platform

The platform shall provide all mandatory functions and services specified in this scope and Annexure A for the full five-year subscription period. Eskom-specific configuration shall not compromise the integrity of benchmarked survey instruments. Benchmark sources, sample bases, dates, sectors, methodology and applicability must be disclosed.

B.2.1. Administrative and framework requirements: role-based access; survey and user administration; confidentiality and anonymity controls; audit logging; data classification and retention; knowledge content; support administration; security monitoring; incident management; and approved future integration capabilities.

Implementation, Transition, and Deployment

The successful bidder shall deliver the complete lifecycle from mobilisation to steady-state service, including governance, discovery, solution design, configuration, data preparation, testing, training, change enablement, launch, go-live, hypercare, operational support and continuous improvement.

The bidder shall prepare and maintain an integrated project plan covering all work packages, milestones, dependencies, resources, deliverables, acceptance points, risks, quality activities and Eskom governance approvals. The schedule must be supplied in MS Project, Excel and PDF formats.

3. **Employee master data used for survey administration shall be loaded, refreshed, validated and securely managed. No historical migration is required initially. Any approved historical data use or future integration shall be governed through Eskom architecture, security, privacy and change-control processes.**

The successful bidder is expected to deliver a comprehensive implementation throughout the entire lifecycle, which includes the following key components:

- The bidder shall deliver change management, communication, training, knowledge transfer, go-live readiness, hypercare, operational handover and an exit plan that guarantees Eskom access to and export of its data.
- The implementation shall accommodate Eskom's scale, geographically dispersed workforce, field operations, diverse employee groups, organisational structure and confidentiality requirements. The rollout strategy must aim to achieve a response rate aligned with industry norms.
- Support for parallel runs, as necessary, to maintain business continuity during the cut-over period.
- Effective change management, along with training and a smooth handover to Eskom's operational teams.

The following baseline volumes apply for sizing and licensing. Employee, line-manager and HR Business Partner figures are based on the end-July 2026 BRS baseline. Line managers and HR Business Partners are included within the employee total.

3.1.1. Employees, including fixed-term contract employees: 43,613.

Line managers: 3,842, included in the employee total.

- HR Business Partners: 338, included in the employee total.
- Enterprise-wide deployment across Eskom Group, divisions, subsidiaries, organisational units, business units, departments and sections, with secure participation from desktop, tablet and mobile devices.
- Integration with multiple upstream and downstream systems, including metering, finance, customer service, and reporting platforms.

- The solution must scale for changes in headcount, organisational structures, survey frequency, concurrent users, reporting volumes, historical records, action plans and future approved integrations.

The service provider shall maintain performance and capacity throughout the five-year term and shall advise Eskom proactively of any licensing, storage or infrastructure thresholds.

3.1.2. Technology Changes During the Contract Term

The bidder shall maintain the solution as a supported, secure and current service throughout the contract term.

- The product roadmap shall cover releases, upgrades, end-of-support dates and migration paths.
- Security patches and updates shall be tested in non-production before production deployment.
- New analytics, automation, AI, accessibility and integration capabilities shall be made available subject to Eskom governance and commercial approval.
- Any change to the platform, business ownership or hosting service provider that could affect the security assessment or assurance status must be notified to Eskom within one month.

At contract expiry or termination, the provider shall support orderly transition and provide Eskom data and agreed artefacts in maintainable, accessible formats.

3.2. Training/Transfer of skills:

The successful bidder shall develop and execute a role-based training, knowledge-management and skills-transfer programme for Eskom personnel involved in survey design, administration, deployment, analytics, reporting, action planning, governance and support.

The programme shall include training plans, user manuals, administrator guides, manager guides, support documentation, attendance records, competency confirmation and effectiveness measures. Knowledge transfer must occur throughout implementation and operations, not only at close-out.

The bidder shall propose final learner numbers, modules, delivery methods and duration during mobilisation. At minimum, the following audiences must be catered for:

Target audience	Training module	Estimated number	Training method / duration
Employee participants	Survey access, confidentiality, participation and support	Up to 43,600	Digital guides, FAQs and accessible just-in-time support

Managers, HRBPs and business users	Dashboards, interpretation, benchmarking and action planning	+/-3,842 managers and +/-338 HRBPs, subject to final role allocation	Role-based virtual/classroom training and practical exercises
Administrators and support users	Configuration, data loading, security, reporting, audit and support	To be confirmed during mobilisation	Instructor-led training, administrator guides and hands-on knowledge transfer

Table 4: Training/Transfer of skills

The training and knowledge-transfer approach shall be reviewed and approved by the relevant Eskom business, Human Capital, Group Technology and training-governance stakeholders.

Training shall be delivered before users assume operational responsibilities and before the applicable survey launch or go-live. Materials shall be supplied in editable and accessible formats.

3.3. Safety:

The Vendor shall comply fully and at all times with all applicable Eskom Health and Safety policies, standards, procedures, and statutory regulations while performing any work related to this project. Compliance shall include adherence to site-specific safety rules, risk assessments, permit-to-work requirements, incident reporting protocols, and the use of appropriate personal protective equipment (PPE).

As part of the onboarding process, the Vendor and all its personnel assigned to the project shall be required to undergo mandatory Health and Safety induction training prior to commencing any work. The induction will cover Eskom's safety standards, site hazards, emergency procedures, environmental requirements, and compliance expectations. Proof of successful completion of the induction shall be submitted to Eskom before access to site or systems is granted.

The Vendor shall ensure that all personnel remain compliant with safety requirements throughout the duration of the project and shall participate in any additional refresher training or safety briefings as required by Eskom. Failure to comply with Health and Safety requirements may result in suspension of work, removal from site, or other contractual remedies as deemed appropriate.

Work may be performed remotely and at Eskom facilities as required for mobilisation, workshops, testing, training, go-live and support. The bidder shall state its on-site assumptions and comply with all access, induction, health, safety, security and confidentiality requirements.

4. Risk Analysis

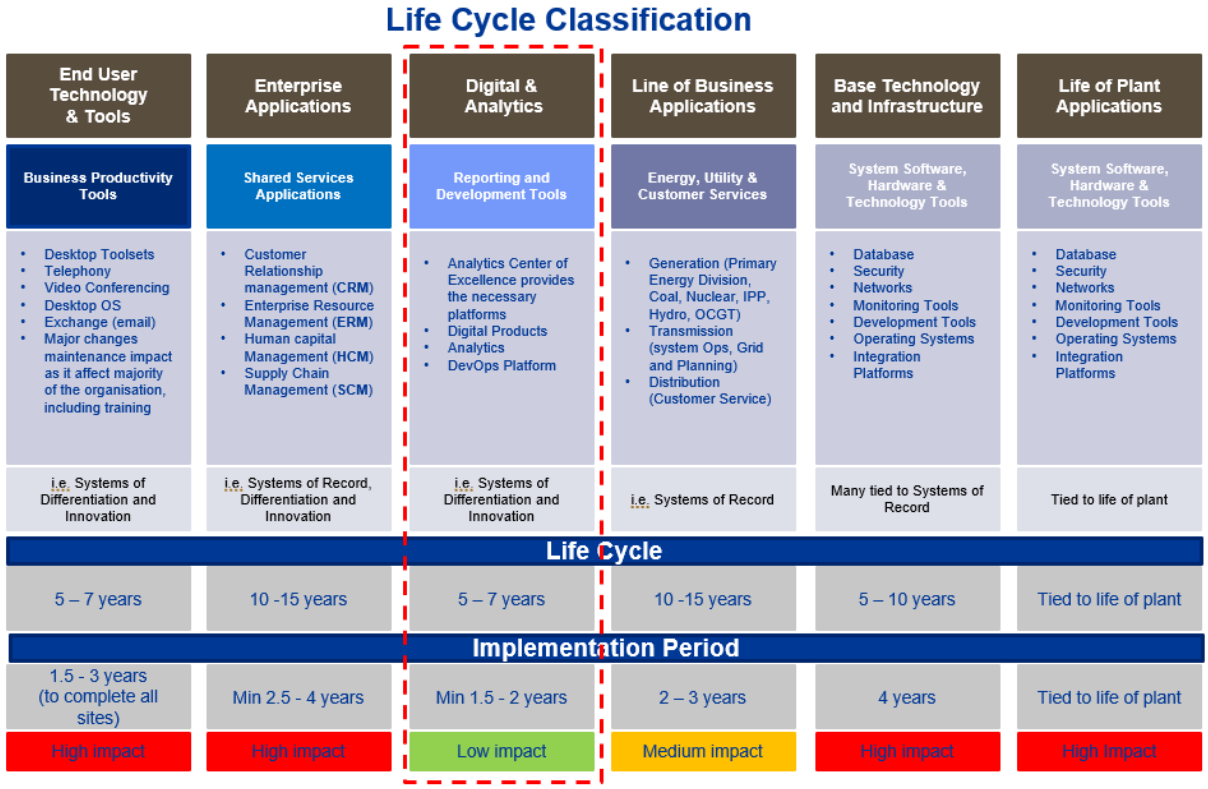
Risk Description	Risk Mitigation	Rating (H/M/L)
Employee trust, confidentiality or anonymity concerns reduce participation – – –	Independent secure platform; approved anonymity thresholds; clear privacy communication; restricted access; auditability; incident response.	High
Participation remains below the minimum target	Multi-channel access; field and non-desk inclusion; PLWD accessibility; reminders; live monitoring; targeted response-rate interventions.	High
Data privacy, hosting, cross-border processing or cyber-security non-compliance	POPIA and Eskom security compliance; ISO 27001; SOC 2 Type II where applicable; encryption; approved data residency; security testing and governance approval.	High
Insufficient adoption of dashboards and action planning	Role-based training; manager guides; change enablement; action templates; adoption metrics; governance and benefits tracking.	Medium

Table 5: Risk Analysis

The bidder shall propose a realistic implementation period and milestone plan covering mobilisation, design, configuration, testing, training, change enablement, launch, go-live and hypercare. The platform subscription and operational service term is five years. Final dates will be baselined after contract award.

5. System Lifecycle Consideration (To be completed by Architecture)

5.1. The contract shall include platform subscription, support, maintenance, security updates, product upgrades, service management, incident management, agreed enhancements, benchmarking updates and continuous improvement for five years. The bidder shall state warranty, hypercare and transition arrangements.



The platform may be unavailable for no more than 24 hours from the business perspective, and recovery must be achieved within one day. The bidder shall propose measurable availability, response, resolution, escalation, restoration, backup, recovery, reporting and service-credit commitments in the SLA schedule.

The bidder shall deliver the implementation and operational service in accordance with the approved baseline schedule and service-level agreement. Milestone completion is subject to Eskom acceptance.

5.2. Development Period for new system/solution

The solution shall remain supported, secure and scalable for the five-year subscription. The product roadmap must address planned releases, support horizons, upgrades, security updates, hosting changes and exit or migration arrangements.

5.3. Support & Maintenance Period

Subscription, support and maintenance for the Employee Voice Platform shall be included in the tendered price for the full five-year term, with all assumptions and optional services clearly separated.

The bidder shall provide go-live hypercare, stabilisation and structured handover to Eskom business and support stakeholders. The duration and resourcing shall be proposed and linked to acceptance criteria.

6. Service Level Agreement requirements

The solution is business essential. The SLA shall support survey launch periods, active fieldwork, reporting cycles and action-planning activities, with heightened support during critical survey windows.

The SLA shall be governed through Eskom service-management and project-governance processes and shall include service reviews, performance reports, incident escalation, root-cause analysis and continuous improvement.
The contract term is five years. Implementation, go-live and stabilisation milestones shall be proposed by the bidder and confirmed in the approved baseline schedule before commencement.

- **Reservation:**

  Eskom reserves the right, at its sole discretion, to leverage its existing enabling agreements with Original Equipment Manufacturers (OEMs) or other approved suppliers for any products, services, or licenses proposed in this tender that can be procured at more favourable terms, including but not limited to price, through these agreements. This includes, but is not limited to, software licenses and related services. By submitting a response to this tender, the bidder acknowledges and agrees that Eskom may exercise this right at its discretion to optimise costs, efficiency, and resource utilisation, in accordance with Eskom’s operational needs.

Annexure A: Mandatory Functional and Business Requirements

Bidders must complete the compliance response for every requirement and identify whether the capability is standard, configurable, requires customisation, is planned, or is not available. Supporting evidence and the relevant proposal reference must be provided.

ID	Grouping	Requirement	Classification	Bidder response / evidence
FR01	Platform	Secure, scalable Employee Voice Platform on a five-year subscription for enterprise-wide listening activities.	Mandatory	
FR02	Anonymity	Anonymous responses and confidentiality controls across reporting, dashboards, analytics and exports.	Mandatory	
FR03	Scale	Digital deployment to approximately 43,600 eligible employees across Eskom organisational areas.	Mandatory	
FR04	Survey types	Enterprise engagement, culture diagnostic, pulse, targeted listening and follow-up surveys.	Mandatory	
FR05	Administration	Authorised configuration of cycles, periods, populations, segments, questions, communications and participation rules.	Mandatory	
FR06	Methodology	Benchmarked frameworks for engagement, employee experience, high-performance culture and approved diagnostics.	Mandatory	
FR07	Customisation	Add Eskom-specific questions without compromising benchmark validity or reporting consistency.	Mandatory	
FR08	Question design	Question libraries, templates, rating scales, open text, branching logic and standard response formats.	Mandatory	
FR09	Statistical quality	Reliability, validity and approved statistical-analysis outputs using documented methods.	Mandatory	
FR10	Channels	Secure web, mobile-compatible and QR-code participation through approved channels.	Mandatory	
FR11	Languages	At least three South African official languages where required and approved.	Mandatory	
FR12	Accessibility	Accessibility for PLWD and compatibility with applicable assistive technologies.	Mandatory	
FR13	Submission controls	Prevent duplicate, unauthorised or invalid submissions while preserving anonymity.	Mandatory	
FR14	Participant experience	Progress indicators, privacy and anonymity notices, completion confirmation and clear accessible messages.	Mandatory	

ID	Grouping	Requirement	Classification	Bidder response / evidence
FR14A	Survey access	Eligible users can securely access assigned surveys during the approved period on desktop, tablet and mobile.	Mandatory	
FR14B	Survey completion	Guided completion, validation, review, save/resume where configured and support for common question types.	Mandatory	
FR14C	Electronic submission	Electronic submission, confirmation, completion timestamp and duplicate prevention.	Mandatory	
FR14D	Communications	Approved invitations, reminders and participation notifications through configured channels.	Mandatory	
FR14E	Segmentation data	Capture authorised organisational and demographic attributes upfront for aggregated reporting only.	Mandatory	
FR15	Dashboards	Real-time role-based dashboards for executives, management, HR and authorised organisational users.	Mandatory	
FR16	Segmentation	Results segmented by approved organisational and demographic dimensions subject to anonymity thresholds.	Mandatory	
FR17	Advanced analytics	Heat maps, key-driver analysis, trend analysis and priority focus identification.	Mandatory	
FR18	Visualisation	Graphical engagement, experience, high-performance, response-rate and benchmark measures.	Mandatory	
FR19	Drill-down	Authorised drill-down to organisational and demographic levels subject to role and anonymity controls.	Mandatory	
FR20	Benchmarking	Relevant South African, international, energy, utility and comparable large-employer benchmarks.	Mandatory	
FR21	Benchmark reporting	Comparisons by index, dimension, organisational segment and approved comparator group, with sources disclosed.	Mandatory	
FR22	Action planning	Create, assign, update, monitor and close action plans linked to survey results.	Mandatory	
FR23	Action tracking	Track owners, due dates, status, completion percentage, overdue actions and follow-ups.	Mandatory	
FR24	Manager guidance	Action templates and recommended interventions linked to themes or priority drivers.	Mandatory	

ID	Grouping	Requirement	Classification	Bidder response / evidence
FR25	Response monitoring	Monitor response rates during active surveys by approved organisational, demographic and channel dimensions.	Mandatory	
FR26	Response improvement	Structured strategy, communications, reminders and interventions to support the targeted response rate.	Mandatory	
FR27	Security and privacy	Encryption, access control, authentication, privacy, incident response and POPIA-aligned processing.	Mandatory	
FR28	RBAC	Role-based access for executives, leaders, managers, OD specialists, HRBPs, employees, administrators and governance users.	Mandatory	
FR29	Audit	Audit logs for access, report access, configuration changes, administration and relevant system activity.	Mandatory	
FR30	Privacy notices	Approved privacy notices, confidentiality declarations, consent messages and anonymity disclosures.	Mandatory	
FR31	Data management	Securely process organisational, demographic, participation, response, comment, metadata, result and action-plan data.	Mandatory	
FR32	Exports	Secure export of approved reports, dashboards, action plans, audit records and artefacts in approved formats.	Mandatory	
FR33	Data sovereignty	Control storage, processing, backup, DR and cross-border processing subject to Eskom approval.	Mandatory	
FR34	Reporting	Provide all reports listed in Annexure B, role-based, exportable and protected by anonymity thresholds.	Mandatory	
FR35	Trends	Compare current and prior cycles where approved historical data is available.	Mandatory	
FR36	Change enablement	Launch communications, employee packs, manager guides, FAQs and escalation guidance.	Mandatory	
FR37	Notifications	Alerts and reminders for participation, deadlines and overdue action plans.	Mandatory	
FR38	Knowledge transfer	Develop and execute skills transfer for design, deployment, reporting, administration and action planning.	Mandatory	

ID	Grouping	Requirement	Classification	Bidder response / evidence
FR39	Documentation	User manuals, training guides, administrator guides and support documentation.	Mandatory	
FR40	Archiving	Retain, retrieve, archive and dispose of records in line with Eskom, POPIA and contract requirements.	Mandatory	
FR41	Recovery	Backup and recovery supporting restoration within one day and a maximum 24-hour business tolerance.	Mandatory	
FR42	Future integration	Capability for future approved integration with identity, repositories, security processes, Power BI, SAP and HC platforms. No direct integration is required initially except for User Authentication where applicable..	Mandatory	
FR43	Future repository export	Secure future transfer of approved records to an Eskom repository for retention, audit or legal purposes.	Mandatory	
FR44	Future identity integration	Future identity and access integration supporting authorised access and RBAC.	Mandatory	
FR45	Future security integration	Future security monitoring and incident-management integration subject to approval.	Mandatory	

Annexure B: Reporting and Dashboard Requirements

ID	Report / dashboard	Minimum content
REP1	Executive Dashboard	Enterprise summary of engagement, employee experience, high-performance measures, response rate and benchmark position.
REP2	Manager / Team Dashboard	Aggregated team results, priority drivers, benchmark context and action status, subject to anonymity thresholds.
REP3	Response Rate Monitoring Report	Participation by Group, division, region, function, demographic and channel during fieldwork.
REP4	Benchmark Comparison Report	Local, international, energy and utility comparisons, benchmark percentile and gap to benchmark, with sources disclosed.
REP5	Heat Map and Key Driver Report	Priority areas, driver strength, risk areas and improvement themes.
REP6	Action Planning Progress Report	Actions created, assigned, completed and overdue, including owner, due date and progress.
REP7	Trend Analysis Report	Current and prior survey-cycle comparisons where historical data is available and approved.
REP8	Access and Audit Report	Authorised users, access events, report access, configuration changes and exceptions.
REP9	Statistical Analysis Report	Reliability, validity, correlation, driver and other approved statistical-quality measures.

Annexure C: Roles and Access Requirements

ID	Role	Access
AR1	Executive Leadership	Aggregated enterprise dashboards, benchmarks, strategic insights and action-plan status.
AR2	Business Unit / Divisional Leaders	Aggregated authorised-area dashboards, benchmarks and action-planning outputs.
AR3	Line Managers	Team-level aggregated results, benchmarks and action planning where anonymity thresholds are met.
AR4	Organisational Development Specialists / SMEs	Approved administrative and analytical access for design, deployment, reporting and action planning.
AR5	HR Business Partners	Approved analytical access for reporting, interpretation and action planning.
AR6	Employee Participants	Secure survey completion and access to participation guidance and summary of results only.
AR7	System Administrators	Approved configuration, user administration, data load and operational support access.
AR8	Information Security / Governance / Audit	Read-only access to audit logs, security evidence and control reports as required.

Annexure D: Required Bid Response

No.	Required submission
1	Executive summary and confirmation of full scope comprehension.
2	Company profile, legal entity details and relevant experience.
3	Solution overview, product roadmap, licensing model and technical architecture.
4	Completed functional, security, technical and service compliance matrices with evidence.
5	Survey methodology, benchmark sources, sample bases, recency, scoring, validity and interpretation approach.

No.	Required submission
6	Implementation approach, response-rate strategy, field and non-desk inclusion, PLWD accessibility and multichannel rollout model.
7	Information security, POPIA, data sovereignty, hosting, architecture, backup, DR and incident-response response.
8	Detailed project plan in MS Project, Excel and PDF with milestones, dependencies, deliverables and acceptance points.
9	Named team, organogram, CVs, qualifications, certifications, role allocation and availability.
10	Support model, SLA proposal, escalation model, maintenance, upgrades, service reporting and continuous improvement.
11	Training, knowledge-transfer, change-management and communication approach.
12	Pricing schedule with five-year subscription, implementation, support, optional services, assumptions and exclusions separated.
13	At least five contactable comparable client references and approved strategy or deliverable examples where client permission exists.
14	Assumptions, dependencies, exclusions, risks, RACI and proposed contract deviations.
15	Signed declarations, certificates, statutory documentation and all returnable schedules.

Annexure E: Minimum Bidder Team

Role	Responsibility	Minimum level
Project Director	Overall delivery accountability, executive engagement and strategic direction.	Partner / Director
Survey Methodology Expert	Survey instrument, scoring model, statistical validity, benchmarks and methodology.	Senior Specialist
Platform / Technical Lead	Configuration, deployment, data, architecture, integrations, security and performance.	Specialist / Expert
Analytics and Insights Lead	Dashboards, key-driver analysis, reporting, insights and benchmarking.	Specialist / Expert
Change and Communication Specialist	Communication packs, manager toolkits, FAQs, adoption and response-rate interventions.	Specialist / Expert
Fieldwork Coordinator	Survey support for field, non-desk and PLWD inclusion across Eskom areas.	Consultant / Coordinator
PMO Coordinator	Schedule, reporting, governance, liaison, quality and document control.	Coordinator

Annexure F: Technical Evaluation Framework

Criterion	Weight	Evaluation focus
1. Functionality / technical solution	35%	Existing tested platform; security, scalability, usability, accessibility and integration capability in comparable organisations.
2. Survey methodology and benchmarking	25%	Validity, benchmark depth, analytics, reporting quality and relevant local and international comparative experience.
3. Implementation approach and project plan	25%	Phased, practical, measurable delivery plan; response-rate strategy; field, non-desk and PLWD inclusion; governance and acceptance.
4. Team qualifications and experience	15%	Director-led multidisciplinary team with relevant organisational culture, survey, technology and comparable large-organisation experience.

Proposals will be scored per criterion using the approved tender scoring guide. The minimum technical qualification threshold is 75 out of 100. The final procurement evaluation methodology and preference-point system will be stated in the issued enquiry documents.

Annexure G: Acceptance Criteria

Acceptance stage	Minimum evidence
Design acceptance	Approved architecture, functional design, security design, data design, configuration workbook, project plan and traceability matrix.
Configuration acceptance	All mandatory functions configured and demonstrated; roles, anonymity thresholds, survey instruments, dashboards, reports and workflows approved.
Test acceptance	Required test cycles completed; traceability achieved; no unresolved severity-one defects; security findings addressed to Eskom acceptance; test closure signed.
Readiness acceptance	Training, communications, support, data preparation, business readiness, go-live, rollback and DR arrangements approved.
Go-live acceptance	Production service available; approved survey launched; monitoring, support and escalation operating; deployment evidence supplied.
Hypercare acceptance	Agreed stability achieved; priority defects resolved; service performance demonstrated; handover completed.
Operational acceptance	SLA reporting, support processes, documentation, administrator capability, data access and continuous improvement operating.
Exit acceptance	All Eskom data, agreed artefacts and transition support delivered in approved maintainable formats; access continuity and secure disposal confirmed.

Annexure H: Data, Retention and Exit Requirements

- All organisational structure data, demographic data, participation records, individual survey responses, free-text comments and information that could identify a respondent are confidential or highly confidential and must be protected by POPIA, Eskom security standards, anonymity thresholds, access controls and approved data sovereignty measures.
- Group Human Capital is the owner of Eskom employee, survey, result, dashboard, action-planning, access and audit information. Third-party benchmark data may remain supplier-controlled, but the source, methodology, recency and permitted use must be disclosed.
- Employee Voice Platform records, survey configurations, aggregated reports, action-planning outputs, audit logs and knowledge-transfer artefacts must be retained for at least seven years and must be retrievable and disposed of in accordance with Eskom requirements.
- At expiry or termination, Eskom must retain access to its data and receive complete exports, documentation and other agreed artefacts in maintainable formats. The bidder shall provide an exit and transition plan and securely dispose of remaining Eskom data when authorised.