

<b>Description of Request</b>	The scope of work outlines the requirements for a work management system to be implemented by Eskom Rotek Industries (ERI)'s business unit: Transformer and Switchgear Services (T&SS). The system should address the company's current challenges, such as inefficient manual processes, lack of centralized task management, and difficulty in generating accurate reports. The system should improve productivity, save costs, and enhance collaboration across departments.
-------------------------------	---

## 1. High level background

Transformer and Switchgear Services (T&SS), a business unit & division of Eskom Rotek Industries, offers maintenance, refurbishment, repair and modification services for transformers and switchgear, both on site and, workshop facilities in Rosherville. On-site transformer services range from loading and off-loading, transporting, installation and commissioning, treatment of oil with mobile oil plants and performing various transformer tests together with technical assessments to determine the condition and general health of the transformer. Testing, servicing, repairs, and replacement is performed in the field on tap-changers, bushings, and auxiliary equipment by trained and experienced site teams.

T&SS is seeking a comprehensive work management solution to address current inefficiencies and enhance operational efficiency. The system must provide robust capabilities for project management, task management, reporting, and integration with existing systems.

### Objectives

- Streamline processes, reduce manual tasks, and enhance productivity.
- Provide real-time data and insights for informed decision-making.
- Foster effective communication and collaboration across departments.
- Adhere to industry standards and regulations.

## 2. Scope of work/Business requirements

### 2.1. The system must provide the following functionalities:

#### Core Features

##### **Project Management:**

Create, manage, and track projects and their associated tasks.  
Define project goals, objectives, milestones, and timelines.  
Allocate resources effectively.

Monitor project progress and identify potential risks.

**Task Management:**

Create, assign, and track tasks.

Set task priorities, due dates, and dependencies.

Capture time and effort spent on tasks.

**Reporting:**

Generate customizable reports on project performance, resource utilization, and task status.

Provide real-time dashboards for key performance indicators (KPIs).

**Integration:**

Integrate with existing systems such as SAP FI, SD, MM, PS, PM, Microsoft Teams, SharePoint, OpenText, Primavera, Mix Telematics, Global Telematics and Lims.

Enable seamless data exchange and workflow automation.

Test equipment software

Time and attendance software

Weather conditions (day and 3 day forecast) software

**Workflow Management:**

Define and automate workflows for various business processes.

Ensure adherence to standard operating procedures (SOPs).

**Customization:**

The vendor should be able to customize the system to meet specific T&SS requirements.

**Scalability:**

The system should be able to accommodate future growth and expansion.

**Mobile Accessibility:**

Ensure the work management system is accessible on mobile devices for field teams to update information and access project data in real-time.

**Disaster Recovery:**

The solution should have a Disaster Recovery option in line with RTO and RPO that will be defined by business.

**Data Migration:**

The solution should take on data from various sources of historical information.

**Information Security:**

The solution will have to adhere to stipulated Eskom Information Security requirements which will be shared with the vendors.

### 2.2. Specific requirements

Requirement Grouping	Requirement
Cloud Based	- Cloud based solution hosted securely within the boundaries of RSA
Azure Tenant Integration	<ul style="list-style-type: none"> <li>- Use Eskom Azure Tenant infrastructure for authentication and authorization, ensuring that only authorized users can access the system and its features.</li> <li>- Seamlessly integrate with the company's existing Azure infrastructure. This integration should allow for: Single sign-on (SSO)</li> <li>- Azure user accounts should be automatically provisioned and deprovisioned in the system when users are added or removed from the Azure directory.</li> </ul>
Project Scheduling	<ul style="list-style-type: none"> <li>- Create detailed project schedules with dependencies and milestones.</li> <li>- Synchronize project schedules with Microsoft Teams/Outlook calendars.</li> </ul>
Risk Management	<ul style="list-style-type: none"> <li>- Capture and assess project risks.</li> <li>- Develop mitigation strategies.</li> </ul>
Time and Attendance	- Automatically capture time and attendance data using biometrics and location services.
Document Management	- Store and manage project documents, including scope of work, specifications, and reports.
Customer Relationship Management (CRM)	<ul style="list-style-type: none"> <li>- Track turnaround time and response time for customer requests.</li> <li>- Streamline the process for sales personnel to create scope of work, estimate costs, and generate quotations.</li> <li>- Store and trace historical data for customer requests.</li> </ul>
Oil Sample Analysis	- Evaluate oil sample analysis results and generate reports with interpretations and recommendations.
Notifications/Alerts	<ul style="list-style-type: none"> <li>- Send email notifications for task activities, approvals/rejections, and escalations.</li> <li>- Enable notifications to be sent directly to team members via email</li> </ul>
Perform Tests	<ul style="list-style-type: none"> <li>- Capture required tests and generate test reports.</li> <li>- Monitor all test results and perform complex calculations based on plant configurations.</li> <li>- Access and analyse historical test data.</li> <li>-</li> </ul>

### 2.3. System Testing

The vendor's testing team is responsible to Acquire the testing requirements, develop the test cases, and conduct testing to ensure that the solution is comprehensively evaluated for implementation in the Eskom IT environment.

The testing staff may not be the same staff as the configuration, development and implementation staff assigned to the Project. The tenderer must make sure skilled adequate resources with an experienced test manager are deployed to test the system.

All testing must be completed on Eskom's test management systems namely Application Lifecycle Management (ALM), Load Runner and Unified Functional Tester (UFT). The deployed testing team is expected to have experience in utilising the said tools.

The testing team must provide unit test results before resuming the next cycle/level of testing as per defined entry and exit criteria outlined in the master system test plan.

A signed off test closure report is required before a test milestone is completed. The following testing and testing milestones must be completed:

Unit Testing – test results from the Tenderer's team.

System Integrated Testing, Functionality testing (in QA – end to end functional testing and integration testing. That means testing with other systems and ensuring that all requirements have been successfully configured). This testing must be driven & executed by the Vendor but must include Eskom staff for completeness & authenticity.

Non-Functional Testing (performance testing and disaster recovery testing). This testing must be driven & executed by the Vendor but must include Eskom staff for completeness & authenticity.

User Acceptance Testing (Testing by the Eskom customer team that the system is working and meets requirements). This testing must be driven by the Tenderer but must be executed by Eskom staff for completeness & authenticity.

The testing team must complete Disaster Recovery Testing on the Disaster Recovery (DR) environment and complete and Vulnerability Testing. The testing team must adhere to the Eskom's TCoE testing standard to be provided as part of the RFP document. All documentation listed in the standards must be produced.

#### **2.4. Non-Functional Security:**

The following are security requirements for the TSS Works Management Solution as a Service (SaaS):

- a) External Third-Party Attestation Reports (Note: SOC reports are only applicable to Cloud Services such as SaaS, PaaS, IaaS and iPaaS, not systems hosted on Eskom's Azure tenant/virtual private cloud (VPC) and on-prem on the Eskom corporate local area network (LAN)/business information network (BIN): SOC 1 Type II and SOC 2 Type II is an attestation standard put forth by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) that addresses engagements undertaken by a service auditor for reporting on controls at organizations that provide cloud services to user entities. The Cloud Service Provider (CSP) shall:
  - i. For all cloud services that store and process financial information and personal identifiable information (PII) including intellectual property (IP), the CSP shall have a valid Service Organisation Control (SOC) 1 and SOC 2 Type II reports, such attestation reports shall be submitted to Eskom for review.

- ii. 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.
  - iii. If the SOC Reports indicate any deficiencies or matters requiring attention, the CSP shall use commercially reasonable efforts to address all such items without any costs to the Eskom.
  - iv. Subject to Section 1.ii, 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 the Eskom at no cost, and such bridging letter shall not cover a period exceeding three (3) months.
- b) The cloud service shall be able to integrate with existing Eskom's on-prem identity provider (IdP), and Multi Factor Authentication (MFA) to enable Single sign-on (SSO).
  - c) Role base access control (RBAC) shall be employed.
  - d) Data at rest (using AES-256) and in transit or in motion (using TLS 1.2, or later version) shall be encrypted.
  - e) Audit trails, logs, user administration and user activity logs shall be enabled, encrypted, and securely kept with limited access to administrators.
  - f) Sensitive information such as personal identifiable information (PII) data in Sandbox/development (DEV) environment shall be masked.
  - g) Incremental daily back-ups shall be done, encrypted, and securely kept offsite.
  - h) Real-time data synchronization or data replication to a secondary or disaster recovery (DR) site, located in different region shall be employed.
  - i) Disaster Recovery Plan (DRP) shall be defined, annually tested and such DRP test results shall be submitted with Eskom Cyber Security team.
  - j) Back up Restore Plan and Procedure shall be defined, annually tested and such test results shall be shared with Eskom Cyber Security team.
  - k) Patch Management Process shall be defined. The software updates and patches shall be tested on Sandbox or development (DEV) environment prior being deployed into production (PROD) environment.
  - l) The static application security test (SAST) and dynamic application security test (DAST) and penetration test shall be conducted prior deploying the cloud system and on-prem systems to PROD, all critical, high, and medium vulnerabilities shall be addressed prior deploying PROD, and the summary of the test results shall be submitted to the Eskom Cybersecurity team for review and acceptance.
  - m) The CSP shall comply with applicable privacy and protection of personal information Acts such as GDPR in European Union (EU) and POPIA in South Africa (SA) where the cloud service is hosted, and the region where the data subjects are physically located.
  - n) The CSP shall notify Eskom immediately or not less than 24 hours when any cyber security breach has occurred. Although the GDPR and the South African Cybercrimes Act 19 of 2020 states that the notification shall be sent within 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.
  - o) 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 the security assessment conducted and the auditor's opinion on the SOC audit.
  - p) The database shall be placed within Eskom corporate LAN/BIN network (if hosted on premise) and partner private network (If hosted in the cloud) behind the perimeter firewall.

- q) Database Security Management tool shall be employed to provide regulatory compliance, encryption, key management, granular access controls, flexible data masking, comprehensive activity monitoring, and sophisticated auditing capabilities.
- r) Distributed Denial of Service (DDoS) protection mechanism shall be employed for all databases.
- s) Web Application Firewall (WAF) for all internet facing applications and/or web-based applications shall be employed.
- t) The Cloud Service shall support the prevailing enterprise services bus (ESB), application programmable interfaces (API's) and Integration Platform as a Service (iPaaS) platforms for security, logging and monitoring for both on-prem, hybrid-cloud and multi-cloud environments such as IBM App Connect, TIBCO Cloud Integration (including Business Works and Scribe), WSO2 Carbon, Software AG web Methods, Neuron ESB, Apache Camel, WebSphere Message Broker, RSSBus Connect, Azure Service Bus and Oracle Service Bus, Salesforce Mulesoft, IBM DataPower, Oracle API Platform, Cyclr, DreamFactory JDBC, Microsoft SQL Server Integration Services (SSIS), SAS Data Integration Studio, Integration Adaptor DirXML, Oracle X AI Services, SAP Business Process Automation, SAP NetWeaver, Oracle Fusion Middleware, Connect Direct, HP Data Protector, WINSCP, FreeFileSync, SAP PI/PO, SAP CPI, HP SOA Systinet, JCAPS, Cloud Pak for Data, K2, Microsoft Power Automate and Zapier but not limited to these listed.
- u) The Cloud Service 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.

**2.5. Licence Management for Maintenance and Support:**

The vendor must provide 100 fixed-user licenses for the system software. Licenses must be valid for 4 years. The vendor must provide 1<sup>st</sup>, 2<sup>nd</sup> & 3<sup>rd</sup> level support services in accordance with the terms of the contract SLA. Licenses must be transferable within the organization.

**2.6. Training/Transfer of skills:**

The vendor will be expected to conduct system user training with training documentation as well system manuals & other relevant supporting documentation.

**2.7. Software Updates and Upgrades**


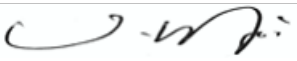
The vendor must provide regular updates and upgrades to the software to ensure compatibility with evolving technologies and industry standards. Upgrades must be made available within N-1 of their release. The vendor must provide a clear upgrade policy outlining the costs and process for upgrading to new versions. The vendor must be open to considering enhancement requests from the client and provide a process for submitting and evaluating such requests.

**3. Deliverables**

The successful vendor will deliver the following:

- A fully functional work management system that meets the specified requirements.
- Comprehensive user training and documentation.
- Ongoing support and maintenance services.

#### 4. Approvals:

End user/Business Requestor:	Name:	Itumeleng Serache
	Designation:	Project Services Manager
	Date:	22 Oct 2024
	Signature:	
ERI Information Management:	Name:	Vicky Mohapi
	Designation:	Business Solutions Manager
	Date:	22/10/2024
	Signature:	
ERI Information Management:	Name:	Tsietsi Madibo
	Designation:	Middle Manager IT Architecture
	Date:	22/10/2024
	Signature:	