




Addendum to SOW: requirements for the Vendor Managed Inventory (VMI) System

Further to the compulsory bidders' clarification meeting held on 27 November 2025, bidders must take note of the following:

- The VMI System will, at a minimum, be implemented as a standalone system.
- The Implementation Plan for this project includes an expectation of integration with Eskom's SAP ERP System, either through SQL-to-SQL integration or via an API. The decision to ultimately proceed with this level of integration is dependent on Eskom Group IT approval of the VMI System.
- Bid pricing should reflect this integration component separately within the Pricing Schedule.
- Eskom reserves the right to implement this SAP integration component of the Project and incur the associated cost.

Bidders are required to submit with their bids the following returnable that indicates the extent to which the bidder is able to meet Eskom's requirements for the software application, treatment and storage of data, disaster recovery, software updates and security testing procedures.

Compiled by	Functional Responsibility	Authorized by
		
Anari Van Greuning JET Office Chief Advisor	Phumlani Ndwandwe JET Office Middle Manager	Dana Gampel Corporate Specialist - JET
Date: 30 November 2025	Date: 01 December 2025	Date: 30 November 2025

VMI System returnable

Bidding company name: _____

Name of VMI System software application: _____

Name of VMI System software owner: _____

Eskom IT System requirements	Please answer "Yes" or "No" to each element
1. Does the System supplier and System currently comply with the following certification and access control requirements?	
a) Valid ISO27001 certificate for the supplier of the application system, where such certification necessarily includes the relevant software product.	
b) Role-based access control (RBAC).	
2. Is the System supplier able to comply with the following data security, audit and activity logging requirements?	
a) Data at rest to be encrypted using at minimum (AES-256), and in transit or in motion using TLS 1.3, or later versions.	
b) Audit trails, logs, user administration and user activity logs shall be enabled, encrypted, and securely kept with limited access to administrators.	
c) Sensitive information such as personal identifiable information (PII) data in Sandbox/development environment (DEV) shall be masked.	
3. Is the Bidder or its System supplier able to comply with the following procedures for data back-ups, synchronisation/replication, recovery and restoration?	
a) Incremental daily back-ups, encrypted, and securely kept offsite.	
b) Real-time data synchronization or data replication to a secondary or disaster recovery (DR) site.	
c) Disaster Recovery Plan (DRP) is defined, annually tested, and results shared with the Eskom Cyber Security team.	
d) Backup Restore Plan and Procedure is defined, annually tested and such test results shared with the Eskom Cyber Security team.	
4. Is the System supplier able to comply with the following software update processes?	
a) Patch Management Process is defined. The software updates and patches shall be tested on Sandbox or Development (Dev) environment before being deployed into production (PROD) environment.	
5. Is the System supplier able to comply with the following Security testing procedures?	
a) The Static Application Security Test (SAST), Dynamic Application Security Test (DAST) and penetration test shall be conducted prior deploying the system into production environment, all critical, high, and medium vulnerabilities shall be addressed prior deploying production environment, and the summary of the test results submitted to the Eskom Cybersecurity team for review and acceptance.	