Description of Request	Procurement of Managed Cloud Services (including professional services, tooling, training, skills/knowledge transfer and day-to-day management of cloud environments) for a period of 6.5 years (78 Months).

1. High level background

Group Information Technology's (Group IT) cloud vision is accelerating Eskom's digital transformation by leveraging the Hybrid multi-cloud journey and innovative new technologies to improve market agility and drive business growth.

A reputable Managed Cloud Services Provider (MCSP) must augment Eskom's cloud management expertise with requisite skills, technology (tools) and methodologies to provide advice and convey best practices. Furthermore, it is to provide the tooling and day-to-day management of a highly dynamic operating environment.

2. Scope of work/Business requirements

2.1. Provide detailed description and volumes of the product/service requested:

2.1.1. Professional / Managed Services

Professional / Managed Services are Required to support the functioning of the Cloud Center of Excellence on an as when basis (some identified roles, but not limited to):

i. Cloud Architecture (including solution, data, security, integration)
ii. Develop overall multi-cloud architecture designs
iii. Develop all other architectural artifacts required to support the multi-cloud environment.
iv. Cloud Operations (including day-to-day management of operations, improvement operations and availability of infrastructure and services, data management)
v. Cloud Security, Risk and Compliance (identification and implementation of the security strategy requirements for effective governance, risk and compliance process management)
vi. Platform Services (management of Hyperscalers and Private cloud environments)
vii. Configuration of applications in the CMP tool once they have been migrated into the prescribed Hyperscalers environments.
viii. Refine the existing Application assessment (6R's) and based on the current workload determine the best Hyperscaler to move the system to and to determine the best deployment options for the workload migration. If this can be done with the use of a tool, then then tool needs to be included in the proposal.
ix. Assist with workload migration to the cloud. This scope item will be used as and when required. Costing will be required based on the expertise used for the execution of migration by providing a resource rate card based on the skill required.

x. The scope items listed above will be viewed as non-committal and will be used as and when required. Costing will be required based on the expertise used for the execution of the tasks by providing suitable resources based on the skills required. In your submission, please include the full list of resources that will work on the Eskom account and specify the level of each resource according to the scales listed below. The rate per resource level must be provided on the pricing schedule only.

Example:

Role	**Role Description**	**Level** (Senior, Intermediate or Junior)
Account Manager		
Cloud Architect		
Cloud Security Architect		
Solution Architect		
Etc.		

Other requirement applicable to professional/managed services:

i. Professional resources must possess cloud certifications from various Hyperscalers, including but not limited to Microsoft Azure, Google Cloud Platform, and Amazon Web Services (AWS).
ii. Eskom resources and key sites are based in Gauteng, the service providers resources may be required to visit Eskom Gauteng sites occasionally. As such, Eskom prefers to work with a tenderer who has a footprint in Gauteng. Tenderers who are based outside of Gauteng will not be reimbursed for travel to Eskom's key sites in Gauteng.
iii. The tenderer will not be reimbursed for travel within the borders of Gauteng.

2.1.2. Provision of a cloud management tool(s)

The service provider must provide cloud management tool(s) which will enable Eskom to manage hybrid and multi-cloud (that is, on-premises, public cloud and edge) services and IT Infrastructure resources. This includes providing:

- Governance,
- Life cycle management,
- Brokering and automation for managed cloud infrastructure resources across multiple functional areas.

Design and Implementation of the tool shall include:
Solution Analysis and Design
Solution Build
Solution Integration
Testing of the solution
Solution Deployment

The cloud management tool(s) will be purchased as a SaaS, with the intention of long-term usage in line with the Eskom system life cycle. Exact volumes will be determined as part of the implementation. The table below describes the current cloud environment.

Environment	Volumes
Number of CMP tool users	86
Number of Virtual Machines	5 500
Number of Databases	839
Storage capacity, across all environments.	9 000 Tb

As part of the design and implementation of the cloud management tool(s) the supplier must develop the architectural detailed design.

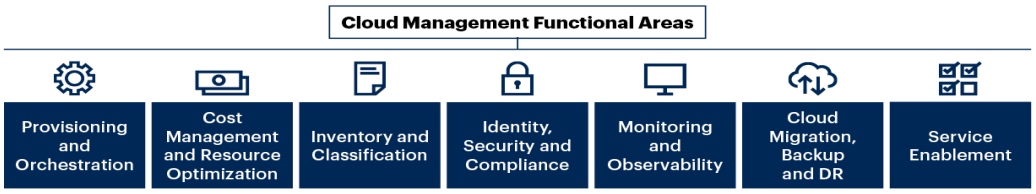
Eskom and service providers resources will use the tool(s) to manage and monitor the hybrid multi cloud environment using the professional/managed services rates described in 3.1.1 above. The service provider resources will work with Eskom resources for a period of 3-5 years using a scaling down approach.

The cloud management tool must be implemented by the cloud management service provider within 12 – 18 months from the contract start date. The implementation must include all integration and configuration required for the tool to operate effectively.

Cloud Management Tool(s) Capabilities

Eskom understands that a combination of tools might be needed to fulfil the functional requirement. It is required that all the tools needed to fulfil the requirements should form part of the proposal. The Cloud management tool(s) must include the following capabilities:

Cloud Management Functionality



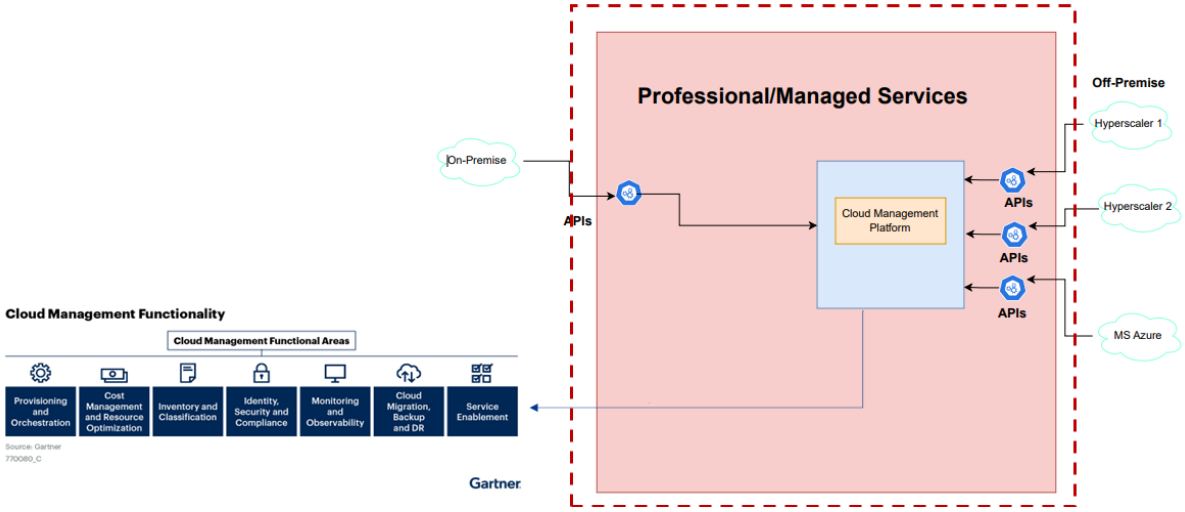
Source: Gartner
770080_C

Gartner

Functionalities	Description
Provisioning and orchestration	Provisioning and orchestration include the tasks to create, modify and delete resources, and to orchestrate provisioning and management workflows.

Functionalities	Description
Service request management	Service enablement includes the tasks to collect and fulfil requests from internal cloud consumers to deploy cloud resources or enable access to cloud services.
Monitoring and analytics	Monitoring and observability include the tasks to monitor health and performance metrics, collect and store logs, generate distributed traces, manage events, and trigger alerts.
Inventory and classification	Inventory and classification include the tasks to discover and maintain an inventory of cloud resources as well as the ability to monitor change and manage configurations.
Cost management and resource optimization	Cost management and resource optimization include the tasks to manage budgets, track and optimize spending, and align capacity to workload demand.
Cloud migration, backup and disaster recovery (DR)	Cloud migration, backup and disaster recovery involve tasks to replicate data to migrate workloads, implement business continuity (BC) or disaster recovery (DR) architectures, or protect data against accidental deletion or malicious activity. This functionality also includes application dependency mapping.
Identity, security and compliance	Identity, security and compliance involve tasks to manage and secure access to cloud services, and to enforce a security configuration baseline.

Solution Context diagram:



Eskom currently operates an Azure Cloud environment alongside several on-premise IaaS environments. These on-premise setups include Eskom Service Provider managed IaaS (Central)across two data centers and Eskom Service Provider-managed regional IaaS across

seven data centers. Additionally, Eskom is in the process of forming relationships with more Hyperscaler Cloud providers.

For this implementation, the tool must facilitate the management of existing environments, specifically on-premise IaaS and Azure IaaS. As Eskom expands to include more Hyperscaler Cloud environments in the future, the cloud management tool(s) will need to integrate with these new environments to ensure seamless management.

Key requirements:

- This solution must be deployed within the borders of South Africa. This includes the total solution (all copies of the data, metadata and any High availability and DR). No data may leave the country.
- The solution must provide consistent management functionality across multiple cloud platforms. Support cloud platform API sets among the major cloud Hyperscalers, including Amazon Web Services, Google Cloud, Microsoft Azure, and VMware etc.

2.1.2.1. Solution Analysis, Design and Build

The scope of the architecture work includes the following key deliverables:

a) Design workshops with business stakeholders to clarify and define in detail business, functional and implementation requirements.
b) Comprehensive documentation for each architecture domain (Data, Solution, Technical, Security, Integration), including diagrams, flowcharts, and textual descriptions as outlined above.
c) High-level presentations to key stakeholders explaining the architecture rationale, design decisions, and benefits.
d) Collaborative sessions and design workshops with the development team to clarify and define in detail non-functional requirements and architectural concepts, and address implementation challenges.
e) Functional specifications document
f) All documents and diagrams to be submitted as digital editable copies (MS Office, MS Visio)

Deliverable Acceptance Criteria:

The architecture work will be considered successfully completed upon approval of the architecture documentation by both Eskom Enterprise Architecture and project stakeholders.

A lead time of at least two weeks needs to be provided for in the timelines to allow for review and approval processes.

- Detailed design approved by Eskom Governance Committee
- Functional specifications documented
- Development environment ready
- Approved Test Plan/Master Systems Test Plan

2.1.2.2. Integration

Please be aware that the Eskom Integration team will do the integration activities. The successful bidder is required to do the business services development to communicate to the other systems.

The application must have the capability of secure communication when exposing the services via the business services.
Additionally, the tenderer must:

- 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 Application Business Services that conform to the specific security and Integration standards.
- Provide Application Business Services that can receive an Integration reply with a full-service response (pre-defined message structure) in case the Application is invoking an Integration Web Service.
- Provide Application Business Services that can communicate via One-Way or Two-Way certificate (SSL/TLS) to secure the channel.
- Provide Application Business Services that support Basic Authentication for Web Services, Database or SFTP for Authentication security.
- Provide Application Business Service with the capability to distinguish between Technical and Business error and handle each one in a separate manner.

2.1.2.3. Testing

The solution will undergo comprehensive testing following Eskom's standards to ensure its completeness and authenticity. The testing team is responsible for gathering testing requirements, creating test cases, and executing the tests to thoroughly evaluate the solution for deployment within Eskom's IT environment.

Please note that the following:

- All testing, except unit testing, will be carried out by the Eskom testing team. The tenderer is responsible for conducting unit testing.
- All testing (including unit testing) must be performed within Eskom's test management systems, such as Application Lifecycle Management (ALM), LoadRunner (for performance testing), and Unified Functional Tester (UFT). The implementation team must coordinate with the testing team to ensure sufficient time is allocated for testing, and that all testing activities are incorporated into the project schedule.
- Before the official test cycle begins, the development team must provide unit test results, adhering to the entry and exit criteria outlined in the master system test plan. A signed-off test closure report is required before marking any test milestone as complete.

The following tests and milestones must be completed:

- **Unit Testing (Development Environment):** Results provided by the tenderer's development team.
- **System Integration Testing & Functionality Testing (QA Environment):** This includes end-to-end functional testing and integration testing, ensuring the solution works with other systems and meets all requirements. The Eskom testing team will lead and execute this testing, while the tenderer's team must provide necessary inputs.
- **User Acceptance Testing (Pre-Prod Environment):** Facilitated by the testing team but executed by Eskom's customer/business team to verify that the system meets the requirements defined in the BRS for completeness and authenticity.
- **Non-Functional/Performance Testing (Pre-Prod Environment):** Led and executed by the performance tester.
- **Disaster Recovery Testing (for the on-premise option).** Led and executed by the Disaster recovery team.

- **Monitoring Testing:** Includes testing for availability, event management and alerting of the tool. Eskom team will lead and execute this testing, requiring the tenderer's team to provide inputs.

All testing requirements must cover all identified interfaces that have been identified. The testing team must adhere to the Testing Centre of Excellence (TCoE) standard document provided as part of the RFP documentation.

Deliverable Acceptance Criteria:

The following artefacts must be produced:

Build, configure & Test:

- Solution technical specifications
- Built solution in the Dev environment (unit testing exit criteria met)
- QA/test and/or Pre-Prod environment prepared for SIT, UAT and performance testing
- Deliverables for turnkey projects in accordance with the testing standard
- Defects raised during the SIT, UAT test cycles addressed
- Tested solution ready to be deployed to the Production environment (Test Closure reports)

Solution Design:

- Solution design artefacts will be required to go to through Eskom governance approvals.

2.2. Security Requirements

The tenderer must be aware of and comply with the requirements listed below.

The following are security requirements for the CMP SaaS tooling:

1. External Third-Party Attestation Reports (Note: SOC reports are only applicable to Cloud Services such as SaaS, PaaS, and IaaS, not systems hosted on Eskom's Azure tenant or virtual private cloud (VPC) and on-prem on the Eskom corporate local area network (LAN) or 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:

    a) 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.
    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 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.

c) Subject to Section 1.b, if tenderer 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.

2. The CMP SaaS shall be able to integrate with existing Eskom's MS (Microsoft)on-prem active directory (AD), Identity (MDI), MS Entra ID, and Multi Factor Authentication (MFA) to enable Single sign-on (SSO).
3. Role base access control (RBAC) shall be employed.
4. Data at rest (using AES-256) and in transit or in motion (using TLS 1.2, or later version) shall be encrypted.
5. Audit trails, logs, user administration and user activity logs shall be enabled, encrypted, and securely kept with limited access to administrators.
6. Sensitive information such as personal identifiable information (PII) data in Sandbox or development (DEV) environment shall be masked.
7. Incremental daily back-ups shall be done, encrypted, and securely kept offsite.
8. Real-time data synchronization or data replication to a secondary or disaster recovery (DR) site, located in different region shall be employed.
9. Disaster Recovery Plan (DRP) shall be defined, annually tested and such DRP test results shall be submitted with Eskom Cyber Security team.
10. Back up Restore Plan and Procedure shall be defined, annually tested and such test results shall be shared with Eskom Cyber Security team.
11. Patch Management Process shall be defined. The software updates and patches shall be tested on Sandbox or development, or non-production environment prior being deployed into production environment.
12. The static application security test (SAST), dynamic application security test (DAST) and penetration test shall be conducted prior deploying the cloud system and on-prem systems to production environment, all critical, high, and medium vulnerabilities shall be addressed prior deploying production environment. The summary of the test results shall be submitted to the Eskom Cybersecurity team for review and acceptance.
13. 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 CMP SaaS is hosted, the region where the data subjects are physically located and where the data is collected.
14. The CSP shall notify Eskom immediately or within 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.
15. The CSP shall notify Eskom in writing 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 SOC report.

16. The database shall be placed within partner private network (If hosted in the cloud) behind the perimeter firewall.
17. Database Security Management tools shall be employed to provide regulatory compliance, encryption, key management, granular access controls, flexible data masking, comprehensive activity monitoring, and sophisticated auditing capabilities.
18. Distributed Denial of Service (DDoS) protection mechanism shall be employed for all databases.
19. Web Application Firewall (WAF) for all internet facing applications and/or web-based applications shall be employed.
20. The CMP SaaS 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, Saleforce 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.
21. The CMP SaaS 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.
22. The CMP SaaS should be capable of integrating with the existing Eskom SIEM tools, including but not limited to Splunk and Sentinel

2.3. Development Period for new system/solution

12-18 Months from contract placement

2.4. Licence Management for Maintenance and Support:

This period will align with the length of the contract.
Lifecycle of the application will be 5-10 Years from going into production.

2.5. Training/Transfer of skills:

The cloud centre of excellence will be staffed with Eskom resources. It is required that the Cloud management service provider support the Eskom resources with professional services of resources with cloud management expertise. The tenderer's resources should at least have Azure certification. While other cloud knowledge will also be required, the specifics are

currently unknown. The personnel should be experienced to provide advice, do transfer of skills and to implement the solution according to best practices.

Transfer of skills should start with the initial implementation and progress over a period of 5 years. Initially most of the day-to-day management of operations will be on the supplier side, but as knowledge transfer and training progress the load should shift to the Eskom resources. Half yearly evaluations of progress will be conducted to assess gaps and any interventions required.

Formal training will be required and will cover the following topics, this training is non-comital and will be requested as and when required:

b) Competence based training for use of the Could Management tool. This is for the Eskom resources who will be working on the tool.

3. Service Level Agreement requirements

- The supplier must meet requirements for the training and knowledge transfer to Eskom resources. Half yearly evaluations of progress will be conducted to assess gaps and any interventions required.
- The implementation of the Cloud Service brokerage must be completed within the agreed time of at least 12 months from the contracting date.
- The business requires 24*7 monitoring of the environment.

Note: Cloud management tooling should have high availability. Specific kpi's for the tooling will be established during implementation. Service penalties will be applied for SLA breaches. The tenderer should allocate 10% of the monthly charges as an at-risk amount.