

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

Description of Request	The Assurance Data Analytics Project aims to implement an Assurance Data Analytics system that automates routine tasks, applies AI/ML to identify risks and patterns, and provides advanced analytics to enhance audit precision for a contract period of 12-months (estimation).
-------------------------------	--

1. HIGH LEVEL BACKGROUND

Enhancement of Business Requirements Specification (BRS) in Response to Technological Advancements (BRS 3380532 - addendum to DEM-02767-L8G0). Given the significant time lapse since the initial request and the continued absence of a suitable analytics solution, recent advancements in the field necessitate the integration of contemporary technologies into the existing Business Requirements Specification (BRS). These enhancements are critical to ensure alignment with current industry standards and to support Internal Audit's evolving analytical needs.

The lack of a modern Assurance Data Analytics tool exposes the organisation to significant operational, financial, compliance, and reputational risks. Manual audit processes are inefficient, prone to human error, and restrict audit coverage to samples rather than entire data populations. This increases the risk of undetected fraud or errors, delayed decision-making, and missed opportunities for strategic insights. Inefficient processes also drive-up costs, limit scalability. This environment is prone to inconsistent methodologies and duplicated effort.

Considering the above, Eskom Internal Audit currently relies on legacy analytics tools that are outdated and no longer supported. The existing environment is characterised by manual processes, limited analytics capability, and restricted access to data insights. This results in inefficiencies, increased risk exposure, and limited audit coverage. The implementation of a modern Assurance Data Analytics solution is required to enable full population data analysis, improve audit effectiveness, and strengthen governance, risk management, and compliance practices.

Impact on Operations:

- Slower audits and delayed insights, impacting executive and operational decision-making.
- Higher fraud and error exposure due to limited detection capability.
- Reduced audit quality, weakening governance and oversight.
- Increased operational risk, with more blind spots in high-risk areas.
- Inefficient use of skilled staff, as manual tasks consume significant time.
- Challenges in attracting and retaining talent, as auditors expect modern digital tools.

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

Due to the complexity of today's business environment, the velocity of change and the impact thereof on organizations, a more integrated and holistic approach to business management and effective safeguard is required.

Currently audits and reviews are performed by various assurance providers either on a planned, ad-hoc, manual or in retrospective view. Key focus areas are planned up front to be reviewed once a year where a sample (+- 5% of population) is selected, majorly based on material values and/or high turnover areas (BU's), which represents a historic period for review. Only reasonable assurance can be provided to management that controls are functioning as intended, only if the sample did not by chance include a possible anomaly. At this stage there is a large volume of unmonitored/undetected possible discrepancies processed daily that could lead to financial loss and/or misstatement of financial and other management information (exception based, not population based, due to too large data volumes).

To address the volumes of transactions, Assurance and Forensic (A&F) together with Process Control and Assurance (PC&A) obtained data analytics tools (sometimes referred to as Computer Assisted Auditing Techniques (CAAT)) and data analytical software called IDEA to assist with trend analysis, data mining, and data analytics for exception identification. However, the software required annual license fees, annual updates, and Eskom only acquired limited licenses. In addition, the IDEA maintenance contract has also lapsed in 2018, with the result that Eskom has not received any software upgrades or updates since then. Furthermore, only two unsupported IDEA licences are currently active within Eskom, and both are linked to a single individual.

The limitation of the current outdated Data Analytics tools is that it is still very labour intensive (manual) and requires dedicated and skilled staff to operate them, and access to the IDEA software is currently restricted to 1 individual. The Data Analytics tool are also run outside any system, which requires a "data dump" of historic transactional data. Discrepancies are then forwarded to representatives for follow up, sometimes in vain as the incidents already incurred long ago, i.e., duplicate payments.

Internal Audit's current Data Analytics capability is constrained and insufficient to meet the growing demand across both IA and the broader Eskom business, primarily due to increasing requirements for advanced analytics and limited resource capacity.

Business motivation & business benefits:

Internal Audit (IA) is responsible for providing independent assurance, investigations, and insights that strengthen Eskom's governance, internal controls, and risk management. The existing system (CaseWare IDEA V10) is outdated, built on obsolete technology, and no longer supported. This limits IA's ability to analyse large datasets, detect risk patterns, and deliver timely, high-quality assurance.

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

Internal Audit currently lacks an Assurance Data Analytics tool that provides Flexible Data Sourcing, automation, workflow integration, Artificial Intelligence (AI), Machine Learning (ML), advanced analytics functionalities and Data Integrity & Security. This gap has been identified as a critical impediment to achieving effective, risk-based, and efficient audit outcomes. The absence of such a tool means reliance on manual processes, limited audit coverage, and slower response to emerging risks. The strategic need for this procurement is underscored by the increasing complexity of the business environment, regulatory expectations, and the necessity to provide timely, data-driven insights to stakeholders.

The time elapsed since the initial request, together with the absence of an appropriate analytics tool, has necessitated the proposal of a new submission for consideration. This delay has exposed a significant capability gap that constrains IA's ability to fulfil its mandate effectively. Implementing a robust assurance data analytics solution is now critical to achieving IA's strategic objective of contributing to a financially viable and sustainable organisation, and to consistently delivering assurance and consulting/advisory services that exceed stakeholder expectations—directly supporting the initiative of **“increased use of Data Analytics.”**

The purpose of this Tender Scope of Work is to procure a modern Assurance Data Analytics Solution for Eskom Internal Audit. The solution shall be delivered as a fully integrated, end-to-end Software-as-a-Service (SaaS) platform that enables automated data ingestion, advanced analytics, and continuous audit capabilities. The Service Provider shall deliver a complete turnkey solution, ensuring that the system is fully operational and ready for use at go-live without requiring Eskom to develop, configure, or operate any core system components.

1. Productivity & Efficiency

- Automates repetitive audit tasks, reducing manual effort
- Shortens audit cycles and accelerates delivery timelines
- Enables auditors to focus on high-value, strategic analysis
- Improves workflow efficiency through standardised processes

2. Risk Reduction & Control Strengthening

- Enables continuous monitoring and real-time alerting
- Detects anomalies, fraud, and control breaches earlier
- Reduces the likelihood and impact of financial and operational risks
- Strengthens overall control environment and governance

3. Enhanced Audit Coverage & Accuracy

- Supports full-population testing (100% coverage vs sampling)
- Eliminates audit blind spots across transactions and systems
- Improves data accuracy and reliability of audit outcomes

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Enables scalable analysis across large and complex datasets

4. Improved Audit Quality & Consistency

- Standardises audit methodologies and procedures
- Reduces human error through automation
- Ensures consistent execution across audit teams
- Enhances credibility and reliability of audit findings

5. Advanced Insights & Strategic Decision Support

- Provides data-driven insights to inform executive decisions
- Enables predictive analytics and trend identification
- Enhances reporting through visual dashboards and analytics
- Supports proactive, forward-looking risk management

6. Operational Efficiency & Compliance

- Drives process improvement across Finance, Procurement, PCA, and operations
- Strengthens regulatory compliance and audit readiness
- Improves turnaround time for audit reporting and issue resolution
- Enhances transparency and accountability across the business

7. Talent Attraction, Retention & Capability Building

- Attracts skilled auditors through modern, digital tools
- Improves employee engagement and job satisfaction
- Supports upskilling in data analytics, AI, and digital audit techniques
- Positions IA as a progressive, technology-enabled function

8. Scalability & Future-Readiness

- Scales easily with increasing data volumes and business complexity
- Adapts to evolving regulatory and audit requirements
- Supports digital transformation and automated business environments
- Future-proofs the audit function with AI and ML capabilities

9. Strategic Positioning of Internal Audit

- Transforms IA into a proactive, data-driven strategic partner
- Enhances stakeholder trust and confidence in assurance outputs
- Strengthens governance and oversight at executive level
- Aligns IA with organisational strategic objectives and priorities

2. SCOPE OF WORK / BUSINESS REQUIREMENTS

2.1. Scope of Work (High-Level)

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

The Service Provider shall deliver a complete turnkey Assurance Data Analytics solution including software provision, hosting, configuration, integration, data ingestion, analytics capability, testing, deployment, training, and support. The solution shall be provided as a SaaS platform with full vendor accountability for delivery and operations.

The successful bidder shall propose a detailed project plan including initiation, configuration, user acceptance testing, go-live, and stabilization phases. Milestones must align with Eskom reporting and audit cycles.

2.2. Business Requirements / Detailed Description

The solution should provide automated data ingestion, advanced analytics, AI/ML capabilities, and continuous auditing with scalability, migration, and transition support.

The contract period is 12 months, aligned to the current mandate, with the understanding that a revised submission will be made to the Group IT Investment Committee (GITIC) once market-related cost estimates have been obtained.

2.2.1 Functional Requirements

The solution shall provide comprehensive data analytics capabilities, including ingestion, processing, and analysis of structured and unstructured data from multiple enterprise systems. The platform shall support flexible data sourcing, advanced analytics, data modelling, artificial intelligence and machine learning capabilities, and configurable dashboards and reporting. The system shall enable real-time monitoring, full population testing, exception detection, and workflow automation to support continuous auditing and assurance activities.

Flexible Data Sourcing

- Support Multi-Source Imports (structured and unstructured data)
- Multi-Source Connectivity: Securely connect and integrate with ERP systems
- Ability to import data via Custom Templates (unstructured data)

Advanced Analytics

- Support advanced analytics, including custom scripting (e.g., Python execution)
- Enable full population testing and complex data interrogation
- Provide real-time and historical data analysis capabilities

Artificial Intelligence & Machine Learning

- Predictive analytics for risk identification and trend forecasting
- Automated anomaly detection and fraud identification

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- AI-assisted audit planning, testing, and reporting

Reporting & Visualisation

- Interactive dashboards and visual analytics for audit insights
- Real-time risk monitoring and exception reporting
- Standardised and custom reporting capabilities for stakeholders
- Drill-down capability and visual analytics

Dashboards & Reporting

- Configurable dashboards
- Drill-down capability
- Real-time and scheduled reporting
- Visual analytics
- Creation of data models for audit and assurance use cases
- Development of dashboards, KPIs, and analytics
- Exception monitoring and risk-based analytics implementation
- ✓ Standard SaaS BI capability

Continuous Monitoring and Automation

- Real-time monitoring of transactions and controls
- Automated alerts and exception reporting
- Workflow automation across audit processes
- Automation of manual audit processes and repetitive tasks
- Workflow orchestration for audit lifecycle management
- Continuous monitoring and automated alerting

Configurable Analytics

- Ability to configure:
 - Rules
 - Thresholds
 - Alerts
 - Monitoring logic
- Ability to define reusable analytics tests
- Optional scripting capability (if part of standard platform)
- ✓ This is configuration, NOT customisation

Data Processing and Analytics

- Advanced data processing, transformation, and modelling
- Support for:
 - Data manipulation and comparisons
 - Statistical analysis
 - Trend identification
 - Exception and anomaly detection
 - Built-in analytics (duplicate detection, anomaly detection, trend analysis)
 - Full-population data testing

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Sampling and statistical analysis
- Data joins, comparisons, and transformations
- Pre-built analytics models
- ✓ Must be provided out-of-the-box (not built by Eskom)

Data Sourcing and Integration

- Collaborate with internal integration stakeholders such as the Integration CoE
- Identify and outline all the required integration points between the application and external systems, services, or APIs.
- Ability to ingest structured and unstructured data from multiple enterprise systems
- Design data exchange formats, protocols, and communication patterns for seamless integration. (SAP, HR, Finance, Procurement, etc.)
- Ensure proper error handling, data consistency, and fault tolerance across integration points
- Integration with Power BI and existing audit/legacy tools
- API development for data extraction from priority systems
- Ability to ingest structured and unstructured data
- Support for APIs, ESB, or iPaaS integration mechanisms
- Automated and scheduled data ingestion
- Application-level integration services (Business Service) API activities to expose/consume and test Services to/from the Eskom Integration Services Bus. Eskom will be responsible for the development of the Integration Services to/from the bus to the internal systems

2.2.2 Non-Functional Requirements

The solution shall meet all non-functional requirements including performance, scalability, availability, and security. The system shall support high availability with defined uptime commitments, disaster recovery capability, and resilience. The solution shall implement role-based access control, encryption of data at rest and in transit, comprehensive audit logging, and compliance with Eskom cybersecurity policies and applicable data protection regulations, including POPIA. The solution shall also ensure maintainability, reliability, and operational sustainability.

High availability and performance

- Collaborate with internal integration stakeholders such as the Integration

Performance Requirements and KPIs

- The solution must meet agreed service levels including system availability, response times, analytics execution time, and user support turnaround
- KPIs will be monitored by Eskom Internal Audit management.

Scalability for users and data

- Initial user base: 50–100 users with scalability for growth

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Eskom requires 90% of the transaction response time for 100 concurrent users to be less or equal to 3 seconds

Security (RBAC, encryption, logging)

- The System shall employ Role-Based Access Control (RBAC) mechanism.
- Data at rest shall be encrypted using at minimum Advanced Encryption Standard (AES)-256 and in transit (or in motion) using at minimum Transport Layer Security (TLS) 1.3 or later version
- The system shall be able to integrate with Eskom's Security Information and Event Management (SIEM) standard technologies such as Syslog, Windows events logging, Simple Network Management Protocol (SNMP), and Application Programming Interface (API) etc.

Disaster Recovery and resilience

- Disaster Recovery Plan (DRP) shall be defined, annually tested, and such DRP test results shall be shared with the Eskom Cybersecurity team only for critical systems

Compliance with POPIA and Eskom standards

- 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

Data Governance, Security and Compliance

- To ensure the Assurance Data Analytics project fully addresses critical security and governance requirements, the following requirements are to be incorporated into the project scope. These requirements form the basis for the evaluation of proposal and selection process.

Requirements which are not adequately considered

Data Management Area	Requirement	Compliance Expectation
Data Sensitivity and Classification	• Bidders must define and apply enterprise-wide data classification for all sensitive information, including	• Bidders must demonstrate how data will be classified, labelled, protected and controlled across production and non-production environments,

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

	PII/PI, financial data and audit data.	including masking of sensitive data where applicable.
Data Sovereignty and Compliance	Bidders must comply with POPIA, data residency requirements and approved cloud hosting regions, including controlled cross-border data transfers.	Bidders must clearly state where data will be hosted, processed and backed up, and must provide controls for lawful transfer, storage and processing of Eskom data.
SaaS Platform Controls	The SaaS platform offered must provide tenant isolation, no data co-mingling, secure backup, restore capability, disaster recovery and vendor breach notification.	Bidders must confirm logical and/or physical segregation of Eskom data, provide evidence of isolation controls, and demonstrate resilience, recovery and incident notification processes.
Data Lifecycle Management	Bidders must define data retention, archiving, export, portability and secure deletion requirements for the full data lifecycle.	Bidders must provide documented lifecycle controls, including retention periods, archiving approach, data return at contract exit and certified deletion of Eskom data when required.

Additional Evaluation Criteria for Bidder Proposals

- **Demonstrate enterprise-wide data classification** for Personally Identifiable Information (PII), financial and audit data, including clear evidence of implementation and practice within the organisation.
- **Provide evidence of customer-managed encryption keys** for protection of sensitive information.
- **Clearly state approved cloud hosting regions** and **cross-border** data transfer controls, demonstrating compliance with all relevant legislation and regulatory requirements.
- **Demonstrate tenant isolation** and no data co-mingling for all SaaS solutions proposed.
- **Detail metadata management practices**, showing alignment with data governance best practices.
- **Submit defined retention and archiving policies**, specifying the approach and timelines for comprehensive data lifecycle management.

Conclusion:

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- These requirements ensure that the Assurance Data Analytics project scope comprehensively addresses security, data governance, and compliance risks. All bidders must demonstrate adherence to these criteria as part of their proposals and will be evaluated accordingly. This addendum is integral to safeguarding Eskom's data and ensuring robust, compliant analytics solutions.

3. DETAILED PRODUCT/ SERVICE DESCRIPTION

Internal Audit (IA) is currently using an old version of CaseWare IDEA software (V10). An IT roadmap indicating the latest technologies was developed and shared with Internal Audit representatives, highlighting, amongst other things, the absence of an Assurance data Analytics tool as a major gap.

These tools are utilised primarily by Assurance Providers including, but not limited to, Internal Audit, Process Control and Assurance (PC&A) and other assurance providers embedded within functions such as Procurement, and Finance, Loss Control. The estimated user base is between 50 and 100 users, with provision for future scalability.

The Business (IA) requires the project to go out on RFP (Request for Proposal) to procure a comprehensive software as a service (SaaS) solution with flexible data sourcing, full automation and workflow capabilities, built-in Artificial Intelligence (AI), Machine Learning (ML) capabilities, advanced analytics functionalities and comprehensive data integrity & security features.

The purpose of this project is to implement an Assurance Data Analytics solution for Internal Audit at Eskom. The solution will enhance Internal Audit's ability to conduct risk-based auditing, continuous monitoring, and data-driven assurance by leveraging automated data pipelines, advanced analytics, and integration with key Eskom systems.

The proposed solution involves the implementation of an Assurance Data Analytics Solution delivered as a Software as a Service (SaaS) platform, specifically designed to enhance internal audit functions. This system will leverage advanced automation, artificial intelligence, and analytics capabilities to streamline audit processes, improve data accuracy, and support more effective risk management. By adopting a comprehensive SaaS solution, the organisation will ensure robust governance and compliance, while also enabling more dynamic and insightful audit activities that align with strategic business objectives.

The Service Provider shall deliver a **fully integrated, end-to-end Assurance Data Analytics solution** as a **Software-as-a-Service (SaaS) platform**, designed to enhance

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

Eskom Internal Audit's capability to perform data-driven assurance, continuous monitoring, and advanced analytics.

The solution shall be delivered as a **complete turnkey capability**, whereby the Service Provider assumes full responsibility for the provision, implementation, operation, and support of the solution, ensuring that the system is fully functional and production-ready at go-live without requiring Eskom to develop, configure, or operate any core system components.

The following will not be accepted as turnkey:

- Partial delivery requiring Eskom to:
 - Design, Build and Implement integration Services on the Approved Middleware Stack
 - Develop dashboards
 - Procure additional tools
- "Platform-only" submissions without implementation
- Reliance on multiple vendors with split accountability
- Solutions requiring Eskom to operate infrastructure

3.1 Solution Overview:

The proposed solution shall:

- Enable automated data ingestion from multiple internal and external sources
- Provide advanced analytics capabilities, including Artificial Intelligence (AI) and Machine Learning (ML)
- Ensure that Eskom data is not used for external AI/ML model training, fine-tuning, or service improvement without Eskom's prior written approval
- Support continuous auditing and monitoring through real-time data processing
- Allow for full population testing, eliminating reliance on sampling
- Deliver interactive dashboards, reporting, and visualisation capabilities
- Support workflow automation and audit lifecycle management
- The solution shall support the transition from manual, retrospective audit processes to a proactive, real-time, data-driven assurance model, improving audit coverage, efficiency, and insight generation

3.2 Cloud SaaS Platform and Hosting Model

The solution shall be delivered as a **true SaaS offering**, with the following characteristics:

- Fully cloud-hosted and vendor-managed platform
 - Vendor-hosted solution
 - Vendor-managed upgrades

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Subscription-based licensing model
- High availability and disaster recovery
- ✓ Confirms “true SaaS”
- All infrastructure, including:
 - Application components
 - Databases
 - Storage and backup
 - Security controls
 hosted within the Service Provider’s secure cloud environment
- The Service Provider shall be responsible for:
 - Hosting and infrastructure management
 - System availability and performance
 - Security and compliance controls
 - Backup, recovery, and disaster recovery
 - Eskom shall not be responsible for hosting, infrastructure provisioning, or system maintenance.

3.3 Integration Requirements

- The solution shall integrate with Eskom enterprise systems including SAP, HR, Finance, Procurement and other data sources through secure APIs and integration platforms. The Service Provider shall ensure data ingestion, transformation, and availability for analytics purposes while maintaining data integrity and security.
- The solution shall integrate with Eskom enterprise systems through secure and standardised mechanisms.
- The Service Provider shall:
 - Identify and define all required integration points
- Design and implement application-level integration services (Business Services) using:
 - REST APIs
 - Web services
- Ensure:
 - Data consistency
 - Fault tolerance
 - Secure data exchange
- The Service Provider shall be responsible for the development and implementation of application-level integration services, while Eskom will manage middleware integration components via the Integration Centre of Excellence (CoE)
- 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.
- The proposed product must have the capability of secure communication when exposing the services via the business services.

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Additionally, the tenderer must:
 - 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 details of the message structure capabilities of the proposed solution. The solution must support integration via a Common Information Model (CIM). Where this is not supported, indicate whether the solution utilises a proprietary message structure (i.e., the application's own business service message format)
 - 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 Basic Authentication 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 errors 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

3.4 Customisation and Configuration

- The solution must:
- Be delivered as a standard SaaS platform
- Support configuration-based flexibility, including:
 - Rules
 - Thresholds
 - Alerts
 - Monitoring logic
- The following will NOT be accepted:
 - Platform-level custom development
 - Modifications to vendor source code
 - Solutions requiring Eskom-led configuration or development

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- The solution must meet requirements primarily through standard functionality, configuration, and supported extensions

3.5 Scalability and Performance

- The solution shall:
- Support an initial user base of approximately 50–100 users, with scalability for future growth
- Support increasing:
 - Data volumes
 - System usage
 - Analytical complexity
- The solution must allow for:
 - True-up (increase) and true-down (reduction) of volumes
 - Expansion of users and capabilities without system redesign

3.6 Implementation, Migration and Transition

- The Service Provider shall deliver full implementation services, including:
- Solution configuration and deployment
- Integration with Eskom systems
- Data migration (where applicable)
- Testing (unit, integration, UAT, non-functional)
- Go-live and stabilisation
- Business Outcomes
- The solution shall enable Eskom Internal Audit to:
- Perform full population data analysis
- Detect anomalies and risks proactively
- Improve audit quality and consistency
- Reduce manual effort and operational inefficiencies
- Provide real-time insights to support decision-making
- Strengthen governance, risk management, and compliance

Roles and Responsibilities:

- Eskom responsibilities include providing access to data sources, business rules, and audit requirements
- The contractor is responsible for solution delivery, configuration, testing, training, and support

3.7 Security and Compliance Requirements

- The solution shall be hosted within the Service Provider cloud environment, with all infrastructure including databases hosted and managed by the vendor. The Service Provider shall implement all required security controls, including encryption, identity and access management, monitoring, logging, vulnerability management, and incident response. The solution shall comply with ISO

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

standards, SOC reporting requirements, POPIA, and Eskom cybersecurity policies. Eskom shall retain full data ownership, and secure data access and export mechanisms shall be provided.

- The Cloud Service Provider (CSP) shall:
 - a) have a valid Service Organisation Control (SOC) 1 and SOC 2 Type II reports, such attestation reports shall be submitted to Eskom for review, if cloud services store and process financial information and personal identifiable information (PII) including intellectual property (IP)
 - b) provide comprehensive summaries of its latest SOC 2 report at no cost upon Eskom's written request once per period of twelve (12) months.
 - c) use commercially reasonable efforts to address all SOC Reports deficiencies, such items without any costs to Eskom
 - d) 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
- Cloud Service Provider shall have a valid Information Security Standard (ISO) 27001, ISO 27017, ISO 27018, ISO 27034 and ISO 15408 certificates
- 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)
- The System shall employ Role-Based Access Control (RBAC) mechanism
- The System shall be able to onboard privileged accounts onto Privileged Access Management (PAM) tools, such as CyberArk but not limited to onboard privileged accounts to securely manage, rotate passwords, monitor, record sessions, control, enforce access to privileged accounts, auditing and reporting capabilities
- Data at rest shall be encrypted using at minimum Advanced Encryption Standard (AES)-256 and in transit (or in motion) using at minimum Transport Layer Security (TLS) 1.3 or later version
- Data shall be secured at minimum using a Secure Hash Algorithm (SHA)-256 for data integrity, securing transactions, and messages
- Audit trails, logs, user administration and user activity logs shall be enabled, encrypted, and securely kept with limited access to administrators
- Sensitive information such as Personal Information (PI) data in non-production environments shall be masked
- Incremental daily back-ups shall be done, encrypted, and securely kept offsite only for all critical systems

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Real-time data synchronization or data replication to a secondary or disaster recovery (DR) site, located in different regions, shall be employed only for critical systems
- Disaster Recovery Plan (DRP) shall be defined, annually tested, and such DRP test results shall be shared with the Eskom Cybersecurity team only for critical systems
- 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
- Patch Management Process shall be defined. The software updates and patches shall be tested in a non-production (DEV/QA) environment before being deployed into the production (PROD) environment
- The static application security test (SAST), dynamic application security test (DAST), vulnerability assessment and penetration test shall be conducted prior deploying the cloud system to production, all critical, high, and medium vulnerabilities shall be addressed prior deploying production, and the summary of the test results shall be submitted to the Eskom Cybersecurity team for review and acceptance
- 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
- The CSP shall notify Eskom immediately or within twenty-four (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 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
- 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 Organization Control's (SOC) audit
- All data storage components, including databases, shall be hosted within the Service Provider's secure cloud environment as part of the SaaS solution. The Service Provider shall be responsible for the provisioning, management, security, backup, and recovery of all database components. Eskom shall not host or manage any database infrastructure within its on-premise LAN/BIN environment
- 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
- Distributed Denial of Service (DDoS) protection mechanism shall be employed for all services

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Web Application Firewall (WAF) for all internet facing applications and/or web-based applications shall be employed
- The Service shall support the application-level integration services (Business Services) Application Programmable Interfaces (API's) as a Service (iPaaS) platforms for security, logging, and monitoring for all on-prem systems
- Cloud Service shall provide e-Discovery with the ability 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
- The system shall be able to integrate with Eskom's Security Information and Event Management (SIEM) standard technologies such as Syslog, Windows events logging, Simple Network Management Protocol (SNMP), and Application Programming Interface (API) etc.

3.8 Technology / Architectural Requirements

- The solution shall be delivered as a Software-as-a-Service platform hosted and fully managed by the Service Provider within a secure cloud environment. All infrastructure components, including servers, databases, storage, backup, and recovery services, shall be provisioned, maintained, and operated by the Service Provider. Eskom shall not be responsible for infrastructure management. The solution shall be scalable and capable of supporting increasing data volumes, users, and analytical workloads.
- SaaS Platform Implementation
 - Configuration and deployment of a secure SaaS analytics platform
 - Scalable and reliable cloud-based architecture
 - Alignment with Eskom IT security and compliance standards
- Architectural Design Cloud SaaS Platform Requirements

A Business Impact Assessment (BIA) review must be done as part of the solution design, together with the business stakeholders and IT Business Continuity team.

Eskom must have a restorable backup copy of the data that can be recovered independently from a cloud service provider.

The diverse nature of workloads must be considered in the design. Different application workloads have unique requirements and considerations. Appropriate placement of workloads must take into consideration factors such as workload characteristics, performance requirements, data sensitivity, and business objectives.

The solution and all components, and workloads and configurations must be continuously monitored. The service provider shall assist to implement the necessary financial management and monitoring processes and enforce agreed limits through available cloud provider policies and governance (e.g., automated business rules, monitoring dashboards). Resource efficiency, optimization, and

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

right-sizing, not only ensure optimised operational expenditure, but also would assist to reduce energy consumption, and contribute to a more sustainable future.

The tenderer is to ensure adherence to Eskom architectural standards as far as possible and where applicable. The following base ICT standards apply – refer to especially the grey shaded standards below: Integration

The cloud offering must efficiently and securely integrate with Eskom’s datacentre at Megawatt Park, the Eskom corporate/ private network(s) and the Enterprise

Integration Platform (IEP or ESB), and in future also with other Eskom approved and deployed multi-cloud/ hyperscale environments (MS Azure tenant already in progress).

Please note that application-level integration services (Business Services) API activities are to expose/consume and test Services to/from the Eskom Integration Services Bus.

Eskom will be responsible for the Analysis, design, development and Implementation of the Integration Services to/from the bus to the internal systems.

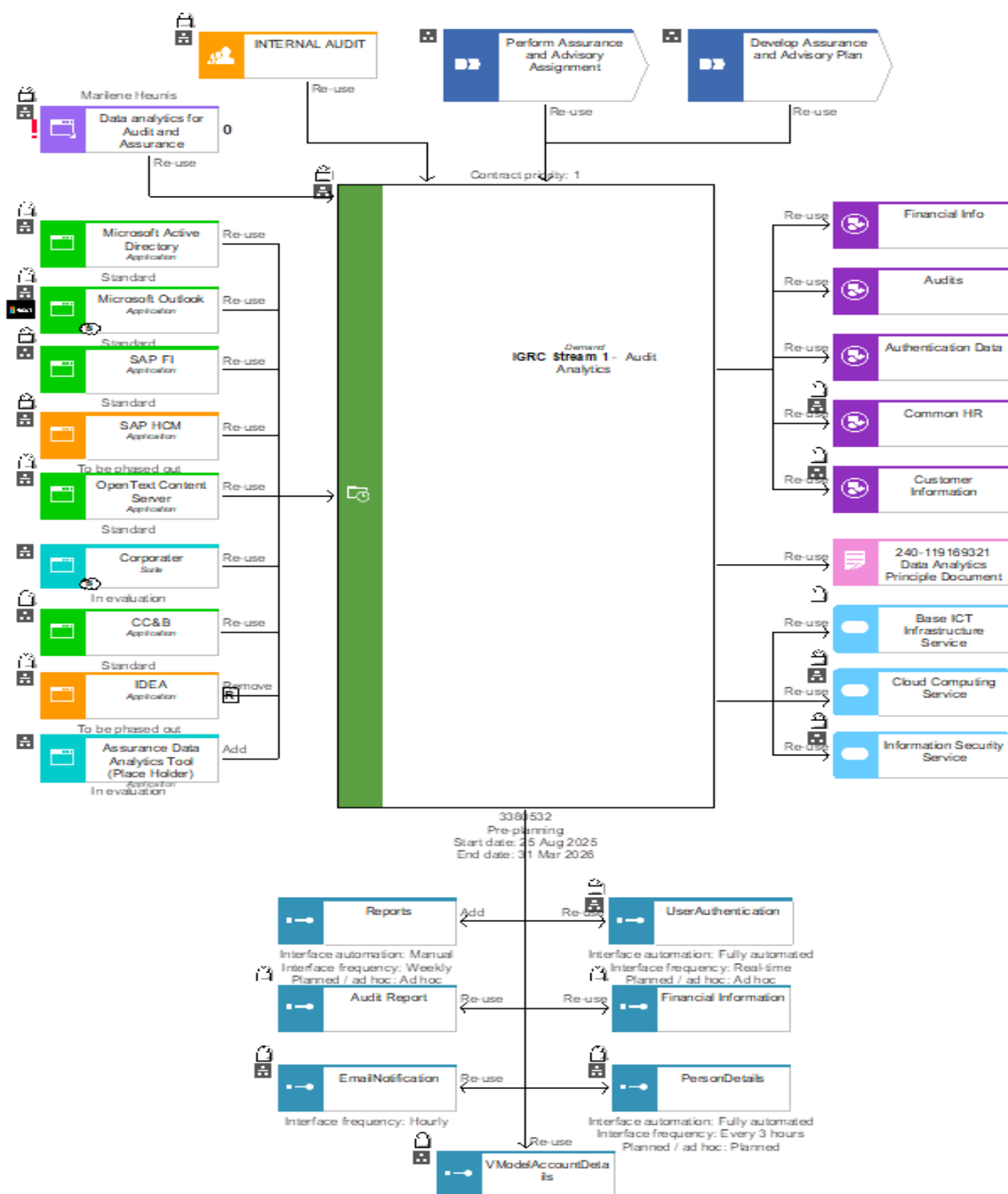
Various integration requirements, which will have to be verified and confirmed during detailed design workshops in the ERA phase.

The Service provider must allow for sufficient time to review the integration requirements with the business, followed by workshops with the Integration CoE.

Integrating with Eskom’s CIPC local data copy/ service will be very important. Efforts are underway to change from the data export provided to an API service.

- Architecture Scope Diagram

The work package scope provides the high-level target architecture components that are expected to be impacted by the architecture engagement. It links the work package to the relevant business, information, application, and technology components that may be impacted.



	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

3.9 IT Standards

Integration	• End interface points, whether consuming or providing, needs to be done in a secure web service fashion. Eskom standard is IBM Cloud Pak for Integration (CP4i) and IBM DataPower Gateway underlying the present Enterprise Integration Platform/ Service Bus.
Authentication	• Azure AD
Database	• MS SQL 2019 • IBM DB2 V 11.5 • Oracle Database 19c (not preferred) • Oracle Database 21c (not preferred) • PostgreSQL V13.2 and PostGIS
Server OS	• Microsoft Windows Server 2022 • SuSe Linux SLES 15 • AIX 7
Client OS	Windows 11
Browser	• Edge • Mozilla Firefox v39 • Mozilla FireFox V60
Load Balancer (ADM)	• F5 Viprion
Backup	• NetBackup
Communication Protocol	• TCP/IP

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

3.10 Licencing Requirements

- The solution shall be provided on a subscription-based licensing model which includes all required functionality, user access, and environments. The model shall support scalability and be fully incorporated into the vendor contract
- Licensing Scope Definition:
The project will define and procure a **subscription-based SaaS licensing model** that aligns to the operational requirements of the Assurance Data Analytics solution
The licensing scope must include:
 - Defined number of users based on business demand
 - User categories, including (but not limited to):
 - Read-only users
 - Analysts
 - Power users
 - Administrators
 - Subscription duration aligned to the contract period
 - Additionally, it must be ensured that:
 - Licensing is fully incorporated into the vendor contract
 - Licences commence at solution go-live
 - Licences adequately cover full operational requirements (not limited to implementation)

NB: The licensing model must ensure that all required platform capabilities are accessible to the relevant user groups in line with their roles and responsibilities.

- Licensing Contract Alignment:
 - The solution licensing model must:
 - Be fully incorporated into the vendor contract and commercial agreement
 - Commence upon production go-live of the solution
 - Provide sufficient coverage for:
 - Implementation validation
 - User adoption
 - Full operational use

NB: Licensing must not be limited to implementation activities only but must support sustained business operations.

- Licensing Impact Considerations:
The following factors must be assessed and addressed during solution definition and procurement:
 - Budget implications based on licence structure and scaling model
 - Dependencies between licensing and project milestones (e.g., onboarding, go-live readiness)
 - Future scalability requirements, including the ability to increase users, data volumes, and functionality

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- SaaS Licensing Checklist (Project-Focused):

Scope and Requirements

- Confirm the solution qualifies as true SaaS (vendor-hosted, managed, and upgraded)
 - Define what is included in the subscription:
 - Analytics platform
 - Dashboards and reporting
 - Data ingestion capabilities
 - Storage
 - Security and access management
- Clearly identify exclusions (e.g. data preparation, advanced modelling, custom development)

- SaaS Licensing Model Requirements:

- The selected solution must provide a clearly defined and transparent licensing model, which may include:
 - User-based licensing (per user or per role)
 - Capacity-based licensing (e.g., data volume, processing capacity)
 - Environment-based licensing (e.g., Production, Test, Disaster Recovery)
- The vendor must:
 - Confirm licensing requirements at go-live
 - Provide options for scaling licensing post go-live
 - Support expansion of users and capabilities without requiring system redesign

- Included Capabilities under Subscription:

- The SaaS subscription must include (as part of the standard offering):
 - Analytics platform functionality
 - Dashboards and reporting capabilities
 - Data ingestion and integration capabilities
 - Data storage and processing capacity (as defined by the vendor model)
 - Security, access control, and audit capabilities

3.11 Testing Requirements

- The solution shall undergo unit, integration, user acceptance, performance, and disaster recovery testing in accordance with Eskom standards. Eskom shall perform integration and acceptance testing while the Service Provider shall perform unit testing and support all testing activities.

Please note 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 (AQM), LoadRunner (for performance testing), and Unified Functional Tester (UFT). The implementation team must coordinate with the testing

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

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 Results provided by the tenderer's development team.
 - System Integration Testing & Functionality Testing. 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. 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. Led and executed by the performance tester.
 - Disaster Recovery Testing (for the on-premises option). Led and executed by the Disaster recovery team.

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.

- The following standard environments must be adhered to:
 1. Development environment
 2. QA/SIT environment
 3. Pre-production environment
 4. Disaster recovery environment
 5. Production environment

NB: Any deviations to the standard environment landscape must be documented and agreed to prior contract award.

3.12 Project Management Requirements

- The Service Provider shall provide project plans, schedules, governance artefacts, and reporting aligned to Eskom PMBOK standards. The solution shall be delivered across the full lifecycle including design, build, integration, testing, deployment, and support.
- Project Management and Governance Artefacts:
 - The Tenderer shall be responsible for providing, maintaining, and executing the following project management, governance, and delivery artefacts and capabilities throughout the duration of the contract.
- Planning and Scheduling:
 - A detailed, integrated project schedule reflecting key milestones, dependencies, and deliverables.

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- A Work Breakdown Structure (WBS) clearly identifying:
 - All fixed-cost deliverables,
 - The cost associated with each deliverable, and
 - The total aggregated cost of all deliverables.

NB: Failure to provide or maintain these artefacts may be considered a breach of delivery obligations and may impact deliverable acceptance and payment milestones.

- Progress Reporting:
 - Weekly progress reports, detailing:
 - Progress against plan,
 - Key achievements,
 - Risks and issues, and
 - Planned activities for the reporting period.
- Commercial and Payment Governance:
 - A comprehensive payment schedule, including:
 - Forecasted payments aligned to deliverables, and
 - Tracking of actual costs against the approved payment schedule.
 - All deliverables shall be priced and invoiced on a fixed-cost basis, unless otherwise expressly agreed in writing by Eskom.
 - Only deliverables that have been:
 - Evaluated by the Eskom Project Manager, and
 - Formally accepted through a Completion and Acceptance Certificate
 may be invoiced by the Tenderer.
- Deliverable Acceptance and Evidence:
 - Delivery Acceptance Certificates, supported by:
 - Documented and approved test results, and
 - Acceptance evidence for each deliverable, in accordance with the agreed acceptance criteria.
- Governance Support and Collaboration:
 - Provision of all information reasonably required by Eskom team members to enable effective governance, oversight, and assurance of the project and its deliverables.
 - Integration of existing Eskom application support teams into the project delivery approach to ensure:
 - Alignment,
 - Knowledge transfer, and
 - Operational readiness.
- Project Management Methodology
 - Eskom follows the Project Management Body of Knowledge (PMBOK) framework, adhering to all knowledge areas, including:
 - Integration
 - Scope

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Schedule
 - Cost
 - Quality
 - Resource
 - Communications
 - Risk
 - Procurement
 - Stakeholder Management
 - And the process groups:
 - Initiating
 - Planning
 - Executing
 - Monitoring and Controlling
 - Closing
- Project Resourcing Transparency
 - The Tenderer must provide full transparency regarding project resourcing, including:
 - 1. Total Effort and Skills**
 - Total estimated man-hours required to deliver the project.
 - A consolidated view of skills and competencies required across the delivery lifecycle.
 - Confirmation that proposed resources collectively meet the project's experience and skill requirements.
 - 2. Delivery Team Structure**
 - The Tenderer must provide:
 - A delivery organogram illustrating the project team structure.
 - Clear reporting lines and accountability.
 - 3. Delivery Team Member Details**
 - A detailed list of all Tenderer team members must be provided, including:
 - Full name
 - Project role
 - Organisation / employer
 - Key responsibilities
 - Relevant skills and competencies
 - Years of relevant experience
 - Certifications and qualifications
 - Estimated effort (man-hours or % allocation)
 - Full-time or part-time allocation
 - Delivery location (on-site, remote, hybrid)
 - 4. Key Resource Assurance**
 - The Tenderer must:
 - Identify key and critical resources,
 - Confirm availability for the project duration, and
 - Describe contingency and replacement plans

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Change Requests and Approval Process
 - All change requests shall be subject to the following approvals:
 - Requester
 - Business Owner
 - Impacted Project Manager
 - Project Delivery Portfolio Manager
 - Project Sponsor
 - Depending on scale or impact, additional approvals may be required.
 - The Project Portfolio Manager will provide guidance on governance and escalation.
 - All approved changes must be formally recorded in Steering Committee minutes.
 - No changes may be implemented without formal approval.
- Software Delivery Lifecycle Alignment
 - The WBS must explicitly reflect the full Software Delivery Lifecycle (SDLC) stages, including but not limited to:
 - Design
 - Build
 - Test
 - Train
 - Deploy
 - Stabilise (post go-live support)
- Tender Response and Delivery Obligations
 - The Tenderer shall provide the following as part of the tender response and ongoing delivery obligations:
 - A clear and explicit list of deliverables and responsibilities excluded from the scope of delivery, to prevent ambiguity and manage scope expectations.
 - A Deliverable Breakdown Structure (DBS) clearly mapping deliverables to pricing.
 - A project schedule that:
 - Identifies all costed deliverables as milestones, and
 - Includes all activities required to achieve each milestone.
 - Disclosure of the applicable resource cost rate(s) to be used in the calculation of:
 - Change requests,
 - Variations, or
 - Additional work.

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Dependencies, Pre-Requisites, and Eskom Inputs
 - The Tenderer must clearly stipulate all dependencies and pre-requisites required from Eskom to ensure successful project delivery. These include, but are not limited to:
 - Access requirements,
 - Integration enablement,
 - Security approvals, and
 - Availability of Eskom stakeholders and systems.
- Project Management and Governance Artefacts:
 - The Tenderer shall be responsible for providing, maintaining, and executing the following project management, governance, and delivery artefacts and capabilities throughout the duration of the contract.
- High-Level Milestones
 - A high-level milestone chart with indicative deliverables will be provided as guidance for tenderers to understand the expected project timelines.

Milestone	Deliverable	Dates - TBC
Project Initiation (Planning)	Deliverable 1 — Obtain all relevant external resource information. Deliverable 2 - Onboarding of the vendors Deliverable 3 – Kick off meeting. Deliverable 4 – Setting up of all project governance forums and project meetings. Deliverable 5 – Analysing the business requirements to ensure clarity of the scope.	
Design	Deliverable 1 — Physical Architectural Design / Deliverable 2 - Functional Specification (PAD)	
Build	Deliverable 1 - Development / Configuration Deliverable 2 – technical specification	
Integration	Deliverable 1 - Build an application-level integration services (Business Services) from “said” systems to “said” systems	NB: ICoE will be responsible for the Analysis, Design and Build of the Service on the Approved Middleware

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

	Deliverable 2 – Adhere to all Integration Centre of Excellence governance forum requirements	stack and are assigning resources to perform the testing internally.
Migration	Deliverable 1 – Migration to “said” system (if applicable)	
Testing	See Output Below per Phase: Deliverable 1 – Unit Testing Deliverable 2 – SIT, Performance Testing Deliverable 3 – UAT	NB: TCoE are assigning resources to perform the testing except for unit testing.

Phase	Input	Output	Responsible Team
Unit Testing		Unit testing Results	Tenderer
System Integration Testing	- Unit testing results - Signed-off test plan - Business test case signs off	Signed Test closure Report	TCOE
Non-Functional	- Performance Test Scripts Sign Off - Signed-off Non-Functional Test plan	- Disaster Recovery report - Penetration Testing report - Performance testing closure report	- DR testing team - Security Team - TCOE
User Acceptance Testing	Signed functional and non-functional Test closure Report	UAT closure report	Eskom business users supported by TCOE

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

Group IT Change Control	Deliverable 1 – Pre-Transfer Report Deliverable 2 – CRMC approvals Deliverable 3 – CIO approval Deliverable 4 – Hand over to Support	
PEOPLE: <i>Training, education, and Skills Development</i>	Deliverable 1 – Training manuals Deliverable 2 – Training and skills transfer	
Finalisation / Close out	Deliverable 1 - Business sign-off Deliverable 2 – Handover to business Deliverable 3 – Commercial operation Deliverable 4 – Close accounts	
Post Implementation Professional Services	Deliverable 1 - Any development / configuration changes (business requirements) to be made by the vendor to the system, post implementation. Deliverable 2 –sustainability and Maintenance on the system.	At Project Managers' discretion

- Intellectual Property and Deliverables Ownership
 - All deliverables produced under this contract shall become the sole property of Eskom, with Eskom retaining full intellectual property and unrestricted usage rights.
 - Deliverables must be provided in a fully maintainable and reusable format, including:
 - Editable documents,
 - Source code,
 - Scripts,
 - Configuration files, and
 - Any additional artefacts required to maintain or replicate deliverables.

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Exit, Close-out and Handover
 - At contract termination or expiry, Eskom must retain access to analytics outputs, reports, and configurations. Knowledge transfer and handover documentation are mandatory.
 - Knowledge Transfer requirements / Documentation deliverables e.g:
 - User manuals / training material
 - Technical documentation
 - Administration guides
 - Configuration documentation
 - Skills transfer
 - Handover
 - Administrator enablement

NB: Failure to clearly articulate these dependencies may result in delivery delays and will be considered during evaluation.

4. TRAINING AND SKILLS TRANSFER

The Service Provider shall deliver training in English by certified facilitators. Training shall include online material, self-paced learning modules, and formal assessments to measure competency. Training must ensure operational sustainability and allow Eskom personnel to support and utilise the solution.

The selected service provider will be responsible for ensuring that Eskom personnel receive adequate training and acquire the necessary technical, functional, and operational skills to effectively support, maintain, and utilise the new Assurance Data Analytics Tool. All training sessions, training materials, and assessments shall be conducted and provided in English. Training content must be clear, professional, and suitable for a business and technical audience. Ensure that all training is conducted by appropriately certified and/or qualified training facilitators.

The training and skills transfer program should promote the long-term sustainability of the solution by minimising reliance on external resources and facilitating effective knowledge transfer to Eskom's internal teams. This will also ensure business continuity after implementation. The approach should encompass structured training, hands-on knowledge transfer, comprehensive documentation, and on-the-job support throughout the implementation lifecycle, as well as during the post-go-live period.

Web-based training for end-users and system support staff. Develop web-based training based on Eskom Academy of Learning (EAL) guidelines. (Users must be able to access web training on and as and when required based). The training can be accessed via the EAL website.

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

4.1. Online Training and Assessment Requirements

The Service Provider shall ensure that all training material and learning content is made available through an online, accessible, and sustainable learning platform, supporting both structured and self-paced learning.

4.1.1. Online Training Content

The Service Provider shall:

- Develop and provide **comprehensive online training material** covering all aspects of the solution (end-user, super user, and technical support roles)
- Ensure training material is **accessible on demand** via an approved digital platform (e.g., web portal or learning management system)
- Include a combination of:
 - User guides and manuals
 - Recorded training sessions and instructional videos
 - Step-by-step tutorials and practical demonstrations

4.1.2. Self-Led Training Capability

The training solution must:

- Enable self-paced (self-led) learning, allowing users to complete training independently
- Be structured into modular learning paths aligned to user roles (e.g., auditor, analyst, admin)
- Allow users to revisit training material at any time to support continuous learning and onboarding of new resources

4.1.3. Formal Training Assessment

The Service Provider shall:

- Provide formal assessment mechanisms as part of the training programme
Include:
 - Knowledge checks (quizzes/tests) per module
 - Practical assessments aligned to real use cases
- Define and communicate minimum competency or pass criteria
- Provide evidence of assessment results, including:
 - Completion status
 - Pass/fail outcomes
 - Attendance and participation tracking

4.1.4. Training Governance and Reporting

The Service Provider shall:

- Track and report on training progress, completion rates, and assessment outcomes
- Provide Eskom with training reports and dashboards
- Ensure training supports auditability and compliance requirements

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

4.1.5. Sustainability Requirement

All training material must:

- Remain available post-implementation for ongoing use Support:
 - New user onboarding
 - Refresher training
 - Knowledge retention within Eskom

4.2. Change Management & Enablement

- User training and upskilling (analytics, AI tools, dashboards)
- Access management and user onboarding
- Change management to support adoption across IA
- Establishment of support and maintenance processes

End users must receive training before the Go-Live. Online User Guides and or videos must be developed to use as a supporting document or guide, when training is conducted for the end and super users.

Any other training (Technical, Functional Support) must start pre implementation, during and post implementation.

Technical Support resources will require a detailed, comprehensive and usable Technical Specification and or a video, developed and signed off for them, to use as a guide or supporting document, during their technical support training.

Functional Support resources will require a detailed, comprehensive and usable Functional Specification and or a video, to be developed and signed off for them, to use as a guide or supporting document, during their functional support training.

The table below is merely example that indicates the possible training needs that Eskom resources may acquire but must be confirmed.

Team:	Training Module:	Number:	Training Type:
End-Users	Full Solution	100 - 200	TEAMS
Super Users	Full Solution	Included in the 200	TEAMS
Support : Technical	Technical Components of the Solution	50 – 100	TEAMS
Support : Functional	Functional components of the Solution	50 – 100	TEAMS

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

5. SERVICE LEVEL AGREEMENT

The Service Provider shall meet defined service levels, including availability, response times, and support. The solution shall provide monitoring, reporting, and continuous service improvement.

5.1. Service Level Agreements

- Uptime $\geq 99.5\%$
- Response & resolution SLAs incidents
- Full support structure and escalation model

The solution shall be delivered as a subscription-based (SaaS) service, with minimum service level requirements aligned to Eskom operational and assurance needs.

5.2 Service Availability

The service must meet the following minimum availability standards:

- Monthly uptime: $\geq 99.5\%$
- Maximum downtime per month: ≤ 3.5 hours
- Planned maintenance: Minimum 72 hours' notice

5.3 Incident Management and Severity Levels

The service provider must support incident management aligned to defined severity categories, including response and resolution targets:

Severity Level	Description	Response Time (MTTR)	Resolution Time (MTTR)
Critical	Service unavailable	≤ 1 hour	≤ 4 hours
High	Major functionality impacted	≤ 2 hours	≤ 8 hours
Medium	Minor functionality impacted	≤ 4 hours	≤ 24 hours
Low	General queries	≤ 1 business day	≤ 3 business days

5.4 Support Services

The service provider must provide:

- Support channels: Email, telephonic, and online portal access
- Support hours aligned to business hours, with optional after-hours support
- Defined escalation procedures for unresolved incidents
- Provide 1st, 2nd and 3rd Line support and maintenance per request over the contract period.
- Telephonic and on-site (when needed) on Software and Hardware (only if service provider provisions hardware)
- Align advisory services with Eskom governance practices

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- 8X5 System Availability, Monday to Friday
- Included in the proposal we are requesting options to be presented to manage the above-mentioned better
- Ensure 8x5 monitoring and 4-hour response is in place to mitigate system downtime
- Ensure the required 3rd and 4th level OEM support is in place

5.5 Performance Monitoring and Reporting

The service provider must:

- Provide monthly service performance reports
- Report on all SLA metrics (availability, incidents, response, resolution)
- Deliver reports within defined timelines following each reporting period
- Provide access to real-time or near real-time service performance dashboards

5.6 SLA Compliance and Penalties

The contract must include mechanisms for:

- Performance tracking against agreed service levels
- Application of service credits or penalties for non-compliance
- Escalation in cases of persistent SLA breaches
- Ten percent (10%) penalty will be imposed if the SLA of 98% availability over a 30-day period is not met.
- A detailed root cause analysis will be done on all incidents before penalties are imposed.
- Planned and agreed downtime and planned maintenance are excluded from the above.

NB: Non-compliance will result in contractual remedies aligned to agreed performance thresholds.

5.7 Review and Continuous Improvement

- The SLA will be reviewed periodically (at least annually or as agreed)
- Service levels may be adjusted based on operational needs and system usage
- Continuous improvement of service delivery is expected over the contract lifecycle

5.8 Maintenance and Support

- As this falls under Digital and Analytics the Support and Maintenance period will be for a 5-year period.

5.8.1 Supplier to provide Support & Maintenance service model e.g.:

- Support Operating Model
- Service Level Agreement (SLA)
- Escalation Matrix

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Resource Support Structure
- Support Process Documentation
- Maintenance & Upgrade Strategy
- Security Patch Management Process
- Incident Response Process
- Disaster Recovery Support Process
- Customer Success / Account Management Model

NB: The above service levels represent minimum baseline requirements. Vendors are expected to propose detailed Service Level Agreements as part of their tender submission, including enhanced service levels where applicable.

“We are defining minimum SLA expectations. Vendors must propose the full SLA as part of the tender — this is standard practice.”

6. EXCLUSIONS

Custom development of core platform functionality and non-SaaS deployment models are excluded.

- No on-prem deployment
- No custom core platform development
- No Eskom-managed infrastructure

The licensing model and solution scope explicitly exclude:

- Custom development of platform functionality
- Bespoke system modifications outside standard platform capabilities
- Any requirement that alters the core SaaS architecture

NB: All required functionalities must be delivered through standard platform features, configuration, and supported extensions.

7. CONTRACT AND COMMERCIAL CONSIDERATIONS

While procurement remains a governance function, the Project Manager must ensure that:

- Licensing is embedded within the primary vendor contract (not treated as an optional component)
- The following are clearly defined:
 - Contract duration (e.g. multi-year term)
 - Renewal conditions
 - Pricing structures and potential annual escalations
- Exit provisions are included, covering:
 - Data export and portability

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Data deletion requirements
- Transition and handover support

8. GOVERNANCE AND COMPLIANCE

Ensure compliance with:

- Eskom data ownership requirements (Eskom retains full ownership of all data)
- Data residency regulations
- POPIA and internal security policies

Confirm vendor capabilities including:

- Audit logging
- Access control mechanisms
- Incident management and reporting

9. ASSUMPTIONS

The solution shall be delivered as SaaS, with available data sources and stakeholder participation.

- SaaS delivery model
- Availability of data sources and stakeholders
- Scalable licensing model

The following assumptions underpin the project scope and delivery:

9.1 Solution Architecture

- The solution will be delivered as a **true SaaS platform** (vendor-hosted, managed, and upgraded)
- Required functionality will be met through **configuration and standard capabilities**, not customisation

9.2 Data Availability and Integration

- Source systems will provide accessible and reliable data
- Integration with key systems (SAP, HR, Finance) will be feasible through standard integration mechanisms

9.3 Data Quality

- Data quality challenges may exist and will require:
 - Implementation of data quality, validation, and cleansing controls
 - Business involvement in validation
 - Enforcement of data governance, security, and compliance frameworks
 - Full audit trails and data lineage tracking

9.4 Licensing and Scalability

- Licensing model will support:
 - Initial go-live requirements
 - Future expansion (users, data, functionality)

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Budget availability will align with licensing requirements

9.5 Resource Availability

- Business and technical SMEs will be available for:
 - Requirements validation
 - Testing and user acceptance
- ICT integration resources will be engaged where required

9.6 Change Management and Adoption

- Users will require training and onboarding
- Successful implementation depends on:
 - Stakeholders buy-in
 - Adoption of new analytics-driven processes

9.7 Governance and Compliance

- Solution will comply with Eskom IT policies, security standards, and governance frameworks
- Procurement will follow formal processes and approvals

9.8 Health, Safety, Security, and Environment (HSSE)

- While primarily a software solution, all on-site activities must comply with Eskom HSSE requirements, including security clearance and information security controls.

10. OUT OF SCOPE

10.1 Development of bespoke analytics engines or modules

- Modification of vendor source code
- Creation of custom system functionality not supported by the platform

10.2 Platform-Level Customisation

- Changes to core system behaviour or architecture
- Re-engineering of vendor-provided workflows

10.3 Bespoke Analytics Development

- Custom-built analytics logic embedded into the platform outside standard capabilities
- Development of unique Eskom-specific algorithms requiring system-level modification

10.4 Non-SaaS Deployment Models

- On-premise hosting of the solution
- Eskom-managed infrastructure or system upgrades

	TENDER SCOPE OF WORK Group Technology	Template Identifier	240-IT042	Rev	2
		Effective Date	April 2023		
		Review Date	April 2028		

- Hybrid models requiring core system ownership by Eskom

10.5 Extensive Custom Build During Implementation

- Vendor-led development of new features as part of implementation
- Treating the solution as a custom software development project

10.6 Integration and Testing

- All testing except unit testing. The tenderer's team is expected to contribute and participate in the testing preparations and executions.
- Integration messages from the Eskom integration bus to Eskom's systems.
- Support and Maintenance of the Eskom Integration Services

NB: The solution must meet Eskom's requirements primarily through standard platform capabilities, configuration, and integration. Custom development of core functionality is explicitly excluded from scope.

11. BUSINESS OUTCOMES (SCOPE ALIGNMENT)

The Implementation will enable Internal Audit to:

- Establish a secure, reliable analytics platform
- Automate data extraction across key business systems
- Ensure trusted, high-quality data for assurance reporting
- Enable dashboards, KPIs, and continuous monitoring
- Reduce manual effort and increase audit coverage
- Improve audit efficiency, insight generation, and governance
- Automated data extraction and ingestion processes
- Use of ESB and iPaaS for secure, scalable data integration
- Reliable, consistent, and near real-time data flows

12. OPERATIONAL CONSIDERATIONS (POST GO-LIVE)

- Define responsibilities for user management (vendor vs Eskom administrators)
- Confirm:
 - SLA and support model
 - System upgrade approach (automatic vs scheduled)
- Ensure licences:
 - Remain valid throughout the operational lifecycle
 - Are sufficient for ongoing business needs
 - Are fully covered contractually beyond implementation