SARS RFP 13/2024

**APPOINTMENT OF A SERVICE PROVIDER FOR THE PROVISION OF ONLINE TRAINING PLATFORM**

Business requirements Specification

**Table of Contents**

[1 Mandatory and Directory requirements 3](#_Toc120872305)

[2 Background 3](#_Toc120872306)

[3 Scope of work 4](#_Toc120872308)

**Business Requirements Specification**

**THE PROCUREMENT OF: Subscription to Online Training Platform for Sars employees**

This document forms part of the RFP pack. The document sets out the business requirements for the procurement of: Subscription to online training platform for SARS employees.

This document and any appendices must be read in conjunction with all other documents in the RFP pack as such documents may contain further requirements that must be considered by the Bidder in compiling a proposal. The Bidder is referred, in particular, but without limitation to the following documents in the RFP pack:

* Main RFP Document
* Technical Evaluation

* 1. **Mandatory and Directory** **Requirements**

Bidders are advised to read the business requirements as set out in this document with care. Where SARS has specified a mandatory requirement, (i.e. where the business requirement, by the context; presence of verbs such as ‘must’; ‘will’; ‘shall’ etc.; or explicit instruction indicates that it is mandatory) the Bidder must build and price its solution accordingly. If a proposal fails to meet or does not address a mandatory requirement, the proposal may, at SARS’s discretion, be disqualified at any stage of the evaluation process as being non-responsive.

Directory requirements (i.e. where the business requirement, by the context; presence of verbs such as ‘may; ‘should; ‘can’ etc.; or explicit instructions indicate that it is directory) are requirements that SARS does not regard as mandatory.

1. BACKGROUND

In support of SARS Strategic Objective number 5, expanding and increasing the use of data, Enterprise Data Management has begun the journey to create the capability of increasing the use of data through analytics, business intelligence, which transforms data into actionable insights. This capability substantively supports the organisation’s strategic intent of voluntary compliance to ensure we provide clarity and certainty where it is needed, make it easy to foster voluntary compliance, collect all revenues due and to detect risks, trends, and instances of non-compliance to enable the organisation to enforce responsibly.

A constraint in giving full effect to SARS Strategic Objective number 5, is the shortage of data analytics skills in South Africa and globally. Recruiting talent that already possess these skills sets is a challenge and it is therefore imperative that SARS upskill internal teams on data topics such as Data Engineering, Data Analysis and Data Science.

The global data environment is constantly changing and the only way to keep abreast with these changes, is to have access to online training platform where contributors (trainers) provide new courses on new topics daily. This will ensure SARS employees have access to quality training.

1. SCOPE OF WORK

SARS requires a subscription to an online training platform that offers a variety of online training interventions for at least 1000 employees per year and not more than 3000 employees over a 3-year period to access at any time. The platform should cover a wide range of topics, including, but not limited to information technology, Data Engineering, Data Analysis, Data Science and Data Management. These topics should encompass both technology-related areas (hardware and software) as well as specific skill sets

3.1 SARS requires the following key features to form part of this online training platform:

* **Extensive Course Library:** With topics ranging from fundamentals in hardware and software to advanced data engineering, machine learning, big data analytics, and cloud computing. This includes courses in Python, SQL, R, data visualization tools, data warehousing, and machine learning algorithms. A non-exhaustive list of topics includes courses like:
* - Data Engineering, Data Analysis, Data Science, Data Architect, Data Stewards
* - Descriptive Analytics, Diagnostic Analytics, Predictive Analytics, Prescriptive Analytics
* - Data Literacy, Data Storytelling and Data Visualisation
* - EDW, Data Lake, Graph Databases, ETL
* - Data Governance DevOps, MLOps, AI Lifecycle, Data Fabric, Data Pipelines
* - SQL, Python, R, Apache Spark, SPSS
* - PowerBI, Tableau, Excel, AWS, Azure, IBM, SAS
* - Machine Learning, Deep Learning, AI, Natural Language Processing, RPA
* **Certifications and Badging:** Industry-recognized certifications and badges on all the topics required by SARS.
* **Skill-Based Learning Paths:** Tailored learning paths that guide learners through a structured sequence, from beginner to advanced.
* **Interactive Labs and Sandboxes:** Real-world scenarios where learners can practice data handling, software usage, and troubleshooting techniques.
* **Analytics and Reporting:** Analytics that track learner progress, completion rates, and skill assessments.
* **Instructor-Led Training (ILT) and Mentorship:** Offer ILT sessions, providing opportunities for questions and answers, mentorship with subject matter experts.
* **Subscription Transferability:** The flexibility to transfer subscription to another user if not optimally utilised.

3.2 SARS requires innovation and trends in online training platform. This includes the following:

* **AI and ML Integration for Personalized Learning:** Incorporate AI-driven recommendations and adaptive learning pathways based on user performance, creating a tailored learning experience.
* **Micro-Learning and Just-in-Time Training:** Offer short, targeted modules that provide flexible, bite-sized learning for professionals to acquire skills on demand.
* **Immersive Learning (VR/AR) and Interactive Labs:** Utilise virtual reality (VR) and augmented reality (AR) technologies to simulate complex technical environments, particularly useful in hardware and systems training.
* **Gamification:** Use of badges, quizzes, and leaderboards to boost engagement, particularly in longer technical courses.

3.3 SARS requires management of online training platform challenges related to:

* **Rapidly Changing Content Needs:** Staying abreast of the fast-paced advancement in IT and data science, ensuring that training content is regularly updated to reflect latest developments.
* **Employee Engagement and Retention:** Overcoming the challenges of motivating employees to complete training programs and retain information, especially in self-paced courses.
* **Measuring ROI and Skills Impact:** Addressing the difficulty of assessing the return on investment (ROI) and practical impact of skills acquired through online learning.

3.4 SARS requires the online training platform to adhere to Information Technology Security Requirements related

to:

SARS require the Service Provider to stipulate whether the components comprising the Service Provider’s solution will be hosted within Service Provider’s own Data Centre, and/or, within a public cloud service. Also, if any component of the Service Provider’s solution makes use of a cloud (SAAS, PAAS, IAAS) service. This should be clearly indicated and described.

Service Provider Personnel Security

The Service Provider will be required to provide details of the Service Provider’s screening and vetting processes of the Service Provider personnel and will ensure that all Service Provider personnel complete the SARS Oath / Affirmation of Secrecy. After terminating the employment of any Service Provider Personnel or transferring such personnel from the SARS account to other work, the Service Provider will eliminate any risk from the Services by, amongst other actions, denying such personnel access to any part of the environment from which the Services are provided to SARS and to inform SARS of such. Service Provider will ensure that the Service Provider Personnel are suitably trained and certified to be able to comply with all information security standards, procedures and best practices set out in this Requirement.

Data Protection and Confidentiality

The Service Provider will not utilise any SARS Data and/or personal information as defined in POPIA of any SARS employee/s for any purpose other than that of providing the Services under this Requirement. The Service Provider will not possess or assert any lien or other right against or to SARS Data. No SARS Data and/or personal information as defined in POPIA of any SARS employee/s, or any part thereof, will be sold, assigned, leased, or otherwise disposed of to Third Parties by the Service Provider or commercially exploited by or on behalf of the Service Provider, its employees or agents. SARS may at any time on written request to the Service Provider require that the Service Provider immediately return to the SARS or destroy any SARS Data and/or personal information as defined in POPIA of any SARS employee/s and may, in addition, require that the Service Provider furnish a written certification to the effect that upon such return it has not retained in its possession or under its control, either directly or indirectly, any such SARS Data or material and/or personal information as defined in POPIA of any SARS employee/s. The Service Provider will implement on or before the Effective Date, and thereafter maintain, appropriate safeguards against the unauthorised access to, and destruction, loss, or alteration of, the SARS Data and/or personal information as defined in POPIA of any SARS employee/s in the Service Provider’s possession which safeguards are: (i) acceptable to SARS, and (ii) no less rigorous than the most rigorous of the practices maintained by SARS or the Service Provider as of the Effective Date. The Service Provider will during its execution of the Services, engage with 3rd Parties, and during such engagements, acknowledges the great importance of the Confidential Information to the Disclosing 3rd Party and, where applicable, Third Party proprietors of such information, recognises that the Disclosing Party and/or Third Party proprietors may suffer irreparable harm or loss in the event of such information being disclosed or used otherwise than in accordance with this Requirement. In this regard each Party will maintain the confidentiality of the other Party’s Confidential Information, using at least the same efforts as it uses to maintain the confidentiality of its own Confidential Information, and as otherwise required under applicable law (POPIA), the terms of this Requirement and the SARS Oath of Secrecy.

The Service Provider will not disclose or publish any Confidential Information in any manner, for any reason or purpose whatsoever without the prior written consent of SARS and provided that in the event of the Confidential Information being proprietary to a Third Party, it will also be incumbent on the Receiving Party to obtain the consent of such Third Party. The Service Provider not to utilise, employ, exploit or in any other manner whatsoever use the Confidential Information for any purpose whatsoever without the prior written consent of the Disclosing Party and provided that in the event of the Confidential Information being proprietary to a Third Party, it will also be incumbent on the Receiving Party to obtain the consent of such Third Party. The Service Provider will restrict the dissemination of the SARS Confidential Information and/or personal information as defined in POPIA of any SARS employee/s to only those of its Staff members who are actively involved in activities for which use of Confidential Information is authorised and then only on a "need to know" and “least-privilege” basis and the Receiving Party will reasonably initiate, maintain and monitor internal security procedures to prevent unauthorised disclosure by its Staff prior to giving any Staff, access to any Confidential Information; and to take all practical steps, both before and after disclosure, to impress upon its Staff who are given access to SARS Confidential Information and/or personal information as defined in POPIA of any SARS employee/s, the secret and confidential nature thereof. The Receiving Party will protect the Confidential Information in the manner, and with the endeavour, of a reasonable person protecting their own Confidential Information. In no event will the Receiving Party use less than reasonable efforts to protect the confidentiality of the Confidential Information.

Data residency

SARS require the Service Provider to indicate whether the Service Provider services are in part or in whole offered through a Cloud Provider Service. Should the services or part thereof be provided through a Cloud Provider, SARS prefer such Cloud Services be rendered from within the borders of South Africa. Data residency is of critical importance to SARS and therefore should reside within the borders of the Republic of South Africa. Should the Service Provider provide such Cloud Services outside of the Borders of South Africa, the Cloud Service Provider must comply with relevant laws, such as section 72 of the POPIA, SARS must understand to which legal jurisdictions SARS’s data will reside, once that understanding is established, Service Provider should ensure alignment with POPIA, The Service Provider must ensure their service-level agreements (SLAs) with Cloud Service Providers are established and these must be shared with SARS.

Data Sovereignty

The Service Provider must ensure that the legal jurisdictions within which the cloud service provider (CSP) operates are acceptable and not contrary to the laws of the Republic of South Africa. SARS must ensure that the legal jurisdictions within which CSP resides are acceptable and not contrary to the laws of the Republic of South Africa.

Data Security

The Service Provider must ensure that their information security strategies, and Policies comply and align with the ISO/IEC 27000 family of standards. Data security solutions to be provided by the CSP must be commensurate with data classification tracking, protection, and encryption.

Data Encryption

SARS will require the Service Provider to utilise International best practices in providing the secure web services, and in this regard would require the use of the latest protocol version of Transport Layer Security (TLS 1.3) as it relates to encryption in-transit of Internet communications. SARS will require the Service Provider to utilise International best practices in providing the secure storage of confidential information by means of encryption at-rest and including Full Disk Encryption (FDE) technologies used. The Service Provider will provide further details of FDE technologies used in relation to server and storage hard drives. SARS desires to use the Service provider’s Key Management Services for the storage of encryption keys as it relates to the services. The Service Provider will be required to provide details of such Encryption Key Management Services (KMS) to ensure compliance to ISO 27000 set of standards and International best practices.

Data Privacy

The Service Provider must be aware of its data privacy obligations when transferring data (including personal data) into the CSP environment in accordance with the POPI Act principles of compliance on data privacy. The Service Provider must regularly review privacy of SARS information, and a report must be provided to SARS on a quarterly basis. The Service Provider through its CSP, must monitor and ensure that the collection, processing, storage, transmission, use and disposal of information (including personal) occurs in line with the POPI Act & Electronic Communications and Transactions Act (ECTA) and According to PAIA requirements on cloud computing. If the privacy of data has potentially or been compromised while in the Service Provider and/or CSP cloud environment, the Service Provider must inform SARS of such incident, such reporting must include details of the nature, extent, and details of data compromised and in according of the provisions of the POPIA, Notification of Security Compromises. The Service Provider must ensure that the contract with the CSP includes clear provisions for the deletion/ disposal/ erasure of data (including personal information). Such deletion or erasure shall be done with SARS authorisation and in a responsible and secure manner by the CSP after consultation and agreement with SARS. SARS will require the CSP provide SARS with a certificate of proof that such data disposal.

Risk Management

The Service Provider must undertake a comprehensive risk assessment of all relevant aspects of the Service Provider computing service being provided prior to the commencement of the SARS services. The risk assessment approach should consider or follow the following:

* ISO 31000 Risk management – Principles and guidelines;
* ISO/IEC 27018; and
* Other relevant regulatory requirements, i.e., POPI, Consumer Protection Act (CPA) add other relevant legislation.

The Service Provider must provide third party accreditation of the CSP. The Service Provider must constantly monitor whether the CSP environment is audited annually. The CSP must provide SARS with any areas of non-compliance. SARS require the Service Provide to conduct regular audits of the ICT environment comprising the Services rendered to SARS and to inform SARS of any finding that would affect the confidentiality, integrity availability or privacy of SARS information as it relates to the Services. SARS require the Service Provide to provide details of its processes with regards to patch management and malware protection (anti-virus management) as it relates to the Services. This must be in line with International Standard Organisation (ISO), National Institute of Standards and Technology (NIST) and Original Equipment Manufacturer (OEM) standards of best practices. SARS require the Service Provider to perform regular threat and vulnerability assessments to determine any risks within the provider Services and to implemented mitigation measures to prevent any cyber-attacks from taking place.

Records Management

The Service Provider must monitor and ensure that records and data created, stored or managed by the CSP remain accessible and retrievable in order to meet all regulatory requirements for information access as required by the POPI Act, PAIA and other legislation.

Contracting

The Service Provider must ensure the existence of the Cloud Service Level Agreement (Cloud SLAs) to support the contractual relationship with the CSP, where applicable. The Cloud SLA must, where practically possible and applicable, include penalty clauses and some incentives for the parties. The Intellectual Property (IP) of the SARS organisational data in the cloud belongs to the SARS as defined in the contract. The Service Provider must ensure that the CSP is contractually prohibited from using “hosted” SARS data or information for any of the CSP’s advertising or commercial purposes. The Service Provider and CSP must comply and adhere to the laws of the Republic of South Africa and must demonstrate compliance with POPI Act, PAIA, and any other applicable laws.

The Service Provider consents that SARS is the owner of all rights, title, and interest in the SARS organisational data and that all data will be maintained, backed up and secured until returned on termination of the agreement (unless other provisions are made for the migration, transfer, or destruction of the data). The Service Provider will consent that data processing (mining) shall be carried out in a manner provided for by the POPI Act and as authorised by SARS. The Service Provider will provide the actual geographic locations where data storage and processing of SARS data will occur, which must be to SARS’s satisfaction. The Service Provider will provide the jurisdiction which governs the operation of the Cloud SLAs. Contract, and application of privacy, confidentiality, access, and information management laws.

The Service Provider will ensure that data storage and processing is restricted to the specified locations where the regulatory framework and technical infrastructure were agreed to, and to ensure that the Service Provide maintain adequate controls over the SARS data. The Service Provider must demonstrate compliance, including a warranty in relation to security, related storage, and access obligations, and Service Level Agreement (SLA) that include cost and operating requirements of providing service continuation in business critical and non-business critical services when disruptions arise. The Service Provider must provide details of the security provisions relating to the service, consistent with the Service Provider Information Security Policy (and where required, compliance with ISO/IEC 27001).

The Service Provider will ensure that unauthorized access, use and or alteration of the SARS data is prohibited. The Service Provider must provide details of the technical mechanisms and procedures in place to support this restriction (e.g. control of user credentials for authentication, data encryption, information dispersal, data separation, and segregation). The Service Provider must provide details of the technical mechanisms and procedures that prevent data loss (e.g.: contractor/organisation responsibilities and routines for backup, failover or redundancy). The Service Provider must provide details of provisions and procedures for backup, restoration of services and disaster recovery. The Service Provider must provide details of all 3rd party network connectivity as it relates to the Service and must provide details of how secure connectivity is maintained as it related to confidentiality integrity and privacy of SARS users and their information, and; the Service Provider must also provide a seamless web interface through which SARS employees can interact with 3rd party Vendors and retailers.

Cloud Exit Strategy

SARS require the existence of a planned exit in preparation for an end or termination of the contract with the Service Provider and CSP. The Service Provider needs to confirm compliance with SARS requirements in this regard. SARS retains an immediate and ongoing right of access to all SARS organisational data held by the Service Provider and/or cloud service provider. The Service Provider should confirm access to SARS information during termination of Services and as part of the agreed contract exit plan. The Service Provider must guarantee the accuracy, integrity, and reliability of data to ensure the ongoing availability of the data and maintain control over its retention or disposal. SARS require that the Service Provider make provisions for the safe return/transfer of data should the cloud service provider be the subject of a takeover. The Service Provider will be required at the termination of the agreement, to make provisions for the secure transfer of SARS data as it relates to the services, at no additional cost to SARS. Metadata relating to SARS in relation to the administration of the services must be disposed of by the Service Provider and as authorised by SARS. SARS will require the CSP to provide SARS with a certificate of proof that such data disposal was performed in line with the provisions of ISO 27001 Requirements for Data and Asset Disposal, the provisions of the POPIA, and/or the provisions of the GDPR and/or that of the Service Provider own disposal policy, whichever process is most rigorous and acceptable to SARS.

Identity and Access Management (IAM)

IAM is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. The IAM technology controls user access, Single Sign-on (SSO), two factor authentication, multi factor authentication and privilege access management. SARS require the Service Provider provide details of how access control will be managed in relation to user access, SSO, and MFA in terms of performing the services. SARS will also require its Human Resource Department to perform administrative duties and would require privilege access for reasons of reporting and management. This privilege access would require strong authentication, and MFA will be a requirement. The Service Provider should provide detail of these user profiling services. The Service Provider must provide details of role-based access control (RBAC) of Service Provider IT administrative Staff in managing the platform as it relates to the Services. The Service Provider must provide details of how access control activities and associated audit trail information is stored, monitored and managed. SARS require that the IAM technology provides for a secure enrolment process that also incorporate MFA technologies. The Service Provider must provide details of such capability and processes as it relates to the Services. The Service Provider must also as part of the provisions of the POPIA, request explicit consent from the SARS employee upon enrolment, and store such provided consent for future reference and in a manner that is legally acceptable.

Disaster Recovery Plan

SARS require that the Service Provider has Disaster Recovery and Business Continuity Plans in place as it relates to the Services, which conform to SARS’s requirements.

Security Monitoring and Automation

Continued Security Monitoring (CMS) is a threat intelligence approach that automates the monitoring of information security controls, vulnerabilities, and other cyber threats to support organizational risk management decisions. SARS require the Service Provider to provide details of the Service Provider’s capability with regard to security monitoring, incident management and the related control processes and measures implemented (CIRT) in relation to the Services which must conform to SARS’s requirements.

Legislative requirements

* Constitution of the Republic of South Africa, 1996.
* Electronic Communications and Transactions Act, 2002 (Act No.25 of 2002) (ECTA).
* Regulation against the Interception of Communications Act, 2002 (Act No.70 of 2002) (RICA).
* Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) (PAIA).
* The Public Finance Management Act, 1999 (Act No. 1 of 1999) (PFMA).
* National Strategic Intelligence Act, 1994 (Act No.39 of 1994) (NSI).
* Protective Disclosures Act, 2000 (Act No. 26 of 2000).
* Protection of Personal Information Act, 2013) (Act No.4 of 2013) (POPIA).
* Critical Infrastructure Protection Act,2019 (Act No. 8 of 2019).
* General Data Protection Regulation (EU) 2016/679

International Standards Instruments

* Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, IT Governance Institute (2006).
* Convergence of Enterprise, Security Organisations, The Alliance of Enterprise Security Risk Management (2005).
* ISO /IEC 27001:2022 – Information Security– Code of Practice for Information Security Management.
* ISO 31000:2018 Risk Management. National Institute of Standards and Technology (NIST) Standards of Good Practice.