

SARS RFP 53/2018

**THE ACQUISITION, MAINTENANCE, SUPPORT AND
RELATED SERVICES FOR SECURITY ADMINISTRATION
AND REPORTING SOLUTION SUPPORTING Z/OS
SECURITY SERVER (RACF) FOR A PERIOD OF THIRTY
SIX (36) MONTHS**

BUSINESS REQUIREMENTS SPECIFICATION

Table of Contents

1	USAGE OF TERMS IN THIS DOCUMENT	3
1.1	References to Other Documents in the RFP Pack	3
1.2	Glossary Table	3
1.3	Mandatory and Directory Requirements.....	4
2	BACKGROUND	4
3	DETAILED REQUIREMENT	5
3.1	Product Requirement.....	5
3.3	Flexibility.....	6
3.4	Transformation	6
3.5	Accreditation.....	6
3.6	Training	7
3.7	Transition.....	7
3.8	Processes, Procedures, Schedules, Work Practices.....	7
3.9	Service Level Requirements	8
3.10	Service Provider Management Personnel.....	8
4	PROCUREMENT SERVICES.....	8
4.1	Procurement At The Outset Of The Term	8
4.2	Procurement During The Term	9
4.3	Maintenance And Support Services	9
4.4	SARS Site Classification.....	10

SARS RFP 53/2018**Business Requirements Specification****Acquisition, maintenance, support and related services for Security Administration and Reporting Solution for z/OS Security Server**

This document forms part of the RFP 53/2018 pack. The document sets out the business requirements that SARS has for the procurement of the design, architecture, installation maintenance support and related services of a Security Administration and Reporting Solution for z/OS Security Server (RACF).

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 taken into account by the Bidder in compiling a proposal.

1 USAGE OF TERMS IN THIS DOCUMENT**1.1 References to Other Documents in the RFP Pack**

Underlined and italicised names are references (or short names) to other documents in the RFP Pack. The Bidder is referred to paragraph 2.2 of the RFP Main Document for the table of documents and their short names.

1.2 Glossary Table

The capitalised terms in this document appearing in the glossary table below will have their corresponding meanings. The Bidder is referred to paragraph 2.2 of the RFP Main Document for the use and meaning of capitalised terms generally in the RFP pack.

Term	Meaning
Change	Change is defined to include all activities necessary to accomplish the change in the hardware or software of a Device.
CV	Curriculum Vitae
IBM	International Business Machines
Install	An Install is defined to include all activities necessary to accomplish the installation of a device at a location.
MSSP	
PPS&G	Policies, Procedures, Standards and Guidelines
RACF	Resource Access Control Facility
RFP	Request For Proposal
SARS	South African Revenue Service
SARS PPS&G	SARS Policies, Procedures, Standards and Guidelines

SDLC	System Development life Cycle
SMF	System Management Facility
SSA	State Security Agency
TAM	Technical Account Manager
TCP/IP	Transfer Control Protocol/Internet Protocol
z/OS	A widely used operating system for IBM mainframe computers.

1.3 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.

2 BACKGROUND

The primary objective of this RFP is to select and appoint a Reseller, Installer, Implementer and Service Provider that is capable to provide SARS with a Security Administration and Reporting Solution for the IBM z/OS Version 2.02 (and higher) Operating System and Security Server (RACF - Mainframe Access Control Management Solution).

The specific requirements of the solution are set out in this Business Requirements Specification.

The appointed Service Provider will be required to provide services related to the proposed solution.

The Term of the agreement will be for a period of thirty six (36) months.

3 DETAILED REQUIREMENT

3.1 Product Requirement

- Currently SARS utilise a mainframe: Make, IBM 2965-N20, Model, Y03 with 439 MSUs. The Mainframe is soft capped for software licencing management purposes. An IBM Sub Capacity Reporting Tool (SCRT) report is produced on the monthly basis to report usage. Currently the mainframe is soft capped at 330 MSUs and pricing should be based on this usage.
- A Security Administration and Reporting solution for IBM z/OS SECURITY SERVER (RACF) on IBM z/OS 2.02 and higher is required (It is expected that SARS may upgrade the Operating System to the latest version during the term). Provision must be made for the implementation of the following required technical specifications:
 - Security Administration
 - The capability to generate IBM z/OS SECURITY SERVER (RACF) commands from online reports to change the status of the IBM z/OS SECURITY SERVER (RACF) resources contained within such reports, regardless of the number of commands.
 - The capability to execute IBM z/OS SECURITY SERVER (RACF) security commands either in online mode or batch mode, allowing for scheduling of security commands at a predetermined date and time via the batch scheduling system.
 - A daily snapshot of the IBM z/OS SECURITY SERVER (RACF) database to ensure currency and relevance of data to perform administrative tasks.
 - Expert level vulnerability analysis and system auditing capabilities of the zSeries Server.
 - Reporting
 - The capability to produce online and batch reports on a scheduled and ad hoc basis.
 - In the case of all batch reports, compatibility with SARS SMTP to ensure that report distribution takes place without the possibility of tampering, i.e. straight from the IBM z/OS Job Entry Subsystem to the authorised recipient.
 - Best-practice reporting, including but not limited to violations, elevated privileged user activity, excessive password resets, as well as the ability to customise reports to meet legislative/audit requirements.
 - Daily extracts from the IBM z/OS SMF data in order to perform historical activity reporting.
 - In addition to extracting IBM z/OS SECURITY SERVER (RACF) type SMF records, TCP/IP records must also be extracted, and must be correlated with IBM z/OS LU-names (logical unit names) via the solution's standard reporting options in order to provide IP address information.

3.2 Accountability

SARS requires a single Service Provider who will be responsible for the provisioning, implementation and operationalisation of the Security Administration and Reporting Solution for the IBM z/OS Security Server (RACF).

The Service Provider will be accountable for the architecture design and after consultation with, and agreement was obtained from the SARS Technical Services team will be required to certify the implementation of the solution.

The appointed Service Provider will be required to adhere to all approved SARS Policies, Processes, Procedures and Standards.

3.3 Flexibility

During the term of the agreement SARS anticipates it may change the landscape of its infrastructure and configuration and the requirements for the support thereof. SARS therefore retains the right to adapt the scope of equipment and processes to its changing requirements including the right to:

- Include new categories and/or exclude current categories of the equipment hosting the solution;
- Include new manufacturers/brands/models and/or exclude current manufacturers/brands/models of the equipment hosting the solution;
- Increase or reduce the quantities of equipment monitored and supported by the solution; and

Therefore, a bidder must be prepared to contract to provide support services on a flexible basis to accommodate SARS's changing needs.

3.4 Transformation

SARS has no specific and immediate requirement to undertake a major transformation in terms of the technology or processes as part of the services. In the event that SARS undertakes a transformation of technology or process during the Term, the Service Provider may be engaged on a project basis to provide services supporting the transformation.

3.5 Accreditation

The appointed Service Provider must comply with SARS quality standards. Resources employed by the appointed Service Provider who will be responsible to implement and support the Security Administration and Reporting Solution, will be required to adhere to the following minimum requirements:

- Resources must be a specialist in the proposed product as well as proven experience in the z/OS and RACF mainframe environments (CV's, proof of training and/or certification must be attached);
- The Service Provider must have a minimum of two years' experience in implementing a Security Administration and Reporting Solution in an enterprise environment with \pm 15000 users (Please supply 2 contactable references, documentation to verify this, size of implementation, industry, scope, contact information);
- The SARS Oath of Secrecy (OoS) Non-disclosure agreements (NDA) will be required to be completed and signed by the service provider (NDA: sign-off) and the service provider resources (OoS: resource sign-off);

- SA issued Secret Security Clearance. The Security Clearance process for the Service Provider resources will commence after the appointment of the successful Service Provider if requested to do so by SARS, and will be for the cost of the successful Service Provider.

3.6 Training

The Service Provider will be required to provide training to SARS staff as part of the skills transfer plan. This training will provide for a maximum of 4 SARS resources to be trained. The Service Provider must include all training cost in the costing of the bid as well as a training plan.

As and when required by SARS, the Service Provider will be required to provide ad hoc technical training, for example, as part of a project.

3.7 Transition

Implementation

The appointed Service Provider will provide SARS with at least one on-site product specialist resource, responsible for the complete architecture / design, installation and implementation of the required solution. SARS change and release processes will be followed. It is expected that the implementation of the solution will not take longer than six (6) months, including but not limited to development, quality assurance, preproduction and production deployment (It is envisaged that the actual involvement from the specialist will be 14 working days in this 6 month period as and when required). The Service Provider must include all consulting cost in the costing of the bid.

Configuration

At least one full time proposed product specialist resource, involved in the initial project, will be required to support the solution and provide skills transfer for an additional 6 months after completion of the implementation for configuration and optimisation of the solution.

Maintenance and Support

The appointed Service Provider will be required to provide SARS with support services for the duration of the contract.

The appointed Service Provider will be required to provide continuous recommendations for improvement of the solution for the duration of the period, at no additional cost to SARS.

3.8 Processes, Procedures, Schedules, Work Practices

The Service Provider is required to execute the processes, procedures, schedules and work practices developed in accordance with policies, processes, standard and Guides (PPS&G), which will be provided as and when required during the different stages of implementation and operationalisation.

Furthermore, the SARS change management processes will determine when any upgrades or maintenance on the solution can take place. The change management process is linked to the SDLC processes within SARS.

3.9 Service Level Requirements

The service provider must agree to a formal Service Level Agreement (SLA)

The Service Provider must measure, monitor and report on the delivery of the Services against the Service Levels in accordance with the SLA.

3.9.1 Service Levels

3.9.1.1 Break-fix Service Levels

- The Service Provider must acknowledge an incident within 30 minutes of notification.
- The Service Provider will provide SARS the capability to log, track and report on incidents logged at the Service Provider.
- The appointed Service Provider will be required to have a suitably qualified product specialist on site within 2 (two) business hours after notification of an incident, and restoration of services will be required within 8 (eight) working hours.

3.10 Service Provider Management Personnel

The Service Provider must provide a Technical Account Manager (TAM) for the management of the SARS account. The TAM is not required to maintain a presence at a SARS site. SARS may also require the presence of TAM at ad hoc meetings at SARS's premises with reasonable notice. Reasonable notice will be determined taking into account the urgency with which the subject matter of a meeting is to be addressed. No separate charge is to be levied by the Service Provider for the TAM and/or for any time spent by the TAM servicing the SARS account.

The TAM is to hold a position of at least Senior Manager within the Service Provider's organisation to provide an effective escalation point for issues that may arise during the Term. The TAM must have a good understanding of the principles of service management.

4 PROCUREMENT SERVICES

4.1 Procurement At The Outset Of The Term

As indicated in paragraph 2, the objective of this RFP is to select and appoint a single Service Provider to provide SARS with a Security Administration and Reporting solution,

consisting of a design, the implementation of the proposed solution, and maintenance/support of software that will be required for the solution.

The procured solution will include all software identified in the design as agreed by SARS.

Software maintenance and support will be required from the appointed Service Provider for the complete implemented Security Administration and Reporting solution.

The appointed Service Provider will be required to provide SARS with the latest software releases at no additional cost, during the term of the agreement.

4.2 Procurement During The Term

No procurement is foreseen during the Term, except for normal annual licence subscription, maintenance and support renewals.

4.3 Maintenance And Support Services

Software maintenance and support services must be performed by the appointed Service Provider on the installed Security Administration and Reporting solution for a period of three years.

The successful bidder will be required to provide SARS with an Architectural design of a Security Administration and Reporting solution, for consideration and approval.

Maintenance and support services consist of:

- Routine maintenance tasks as defined by the original equipment manufacturer best practices. Upgrades are to be performed timeously, and are included in the annual licence/maintenance fee.
- Break-fix activities. The appointed Service Provider will be required to support all software implemented for the approved solution. Any software outages will be restored within the service levels identified in paragraph 3.9.1 of this document. Restoration will be achieved when hardware and software was restored to the last working configuration, and in accordance with the approved SARS change process.
- Ad hoc services

These services are required to be performed in respect of all services in scope on a project basis and the Service Provider needs to provide a table with applicable rates for these services.

4.4 SARS Site Classification

The management component of the Security Administration and Reporting Solution will be installed in the data centre at SARS Head Office and at the SARS Disaster Recovery site.