**RFI SPECIFICATION** 

COVER PAGE (SUMMARY)

**BIDDERS MUST SUBMIT ANNEXURE 1 TOGETHER WITH THE INVITATION TO BID DOCUMENT**

|  |  |
| --- | --- |
| **RFI No:** | **RFI 2731/2023** |
| **Description** | **REQUEST FOR INFORMATION (RFI) FOR PROVISION OF SOFTWARE CONFIGURATION MANAGEMENT SOLUTIONS FOR Z/OS SOFTWARE DEVELOPMENT** |
| **Publication Date** | **18 APRIL 2023** |
| **Virtual Vendor Briefing Session** | **A Non-Compulsory Virtual Briefing Session will be held as follows:**  **Date: 26 April 2023**  **Time: 11h00 am (South African Time)**  **Venue: Online (Teams)**  **Link:** [**Click here to join the meeting**](https://teams.microsoft.com/l/meetup-join/19%3ameeting_OGU3OWQ1NzMtOGI0ZC00YjE2LTk4ZjktY2E2NzAwMzkwMmNi%40thread.v2/0?context=%7b%22Tid%22%3a%2248cd5724-88c7-48c3-a665-945436edd7fc%22%2c%22Oid%22%3a%22d16c4658-8ada-4d14-9384-5a456245c314%22%7d) |
| **Closing Date for questions / queries** | **05 May 2023** |
| **Proposal Submission Address** | **Proposals will be accepted electronically via the following email address:** [**tenders@sita.co.za**](mailto:tenders@sita.co.za) |
| **RFI Closing Details and Address** | **Date: 11 May 2023**  **Time: 11h00 am (South African Time)**  **Email:** [**tenders@sita.co.za**](mailto:tenders@sita.co.za) |
| **RFI Validity Period** | **N/A** |

**PROSPECTIVE RESPONDENTS MUST REGISTER ON NATIONAL TREASURY’S CENTRAL SUPPLIER DATABASE PRIOR TO SUBMITTING RESPONSES.**

Contents

[ANNEX A: INTRODUCTION 3](#_Toc117951754)

[1. PURPOSE AND BACKGROUND 3](#_Toc117951755)

[1.1. PURPOSE 3](#_Toc117951756)

[1.2. BACKGROUND 3](#_Toc117951757)

[1.3. Objective 4](#_Toc117951758)

[2. Confidentiality 4](#_Toc117951759)

[3. Precedence of documents 5](#_Toc117951760)

[4. Briefing and information session 6](#_Toc117951761)

[5. Submission of documents 6](#_Toc117951762)

[6. TECHNICAL INFORMATION REQUEST ON VULNERABILITY MANAGEMENT SOLUTION 6](#_Toc117951763)

[6.1.1. INTEROPERABILITY 12](#_Toc117951764)

[6.1.2. SPECIAL REQUIREMENTS 12](#_Toc117951765)

[6.1.3. TRAINING 12](#_Toc117951766)

[7. Contact details 12](#_Toc117951767)

[ANNEX B: Terms and definitions 13](#_Toc117951768)

[1. ABBREVIATIONS 13](#_Toc117951769)

1. INTRODUCTION

# PURPOSE AND BACKGROUND

## PURPOSE

The purpose of this Request for Information (RFI) is to invite suppliers (hereinafter referred to as “bidders”) to submit information on Software Configuration Management (SCM) Solution for z/OS Development that can be deployed within the client’s network. This RFI is solely for information gathering purpose and NOT to make a selection or an award. The information collected in this fashion will not be used to lead to sourcing from one supplier only nor will it be used to write the ultimate specification in a matter that would suit just one specific supplier.

SITA is gathering information on what Software Configuration Management (SCM) Solutions for z/OS Development are available in the market, what specifications the products have, the availability of the products in the market place, and the possible indicative pricing and timing of delivery of such solution.

## BACKGROUND

The Client has a well-established Mainframe environment. The ecosystem is comprised of few Applications variants, each with their own purpose stack, that delivers scalable mainframe services to our clients.

Software Configuration Management (SCM) ensures the control of changes to software and provides the capability to revert back to previous versions or releases of modules, should it be required. Without SCM, effective management, tracking and version control of developed application source code cannot be conducted. The client is at risk as application software can be totally lost, if SCM is not applied.

A complete SCM solution consists of many subsystems. These include, but are not limited to, version control, security, auditing, deployment and release management.

## Objective

The respondents to the Request for Information (RFI) are requested to submit detailed information

of software Configuration Management (SCM) Solution for z/OS for developer as per the specifications.

# Confidentiality

1. The information contained in this document is of a confidential nature, and must only be used for purposes of responding to this RFI. This confidentiality clause extends to all respondent(s) or associates whom you may decide to involve in preparing a response to this RFI.
2. For purposes of this process, the term “confidential information” shall include all technical and business information, including, without limiting the generality of the foregoing, all secret knowledge and information (including any and all financial, commercial, market, technical, functional and scientific information, and information relating to a party’s strategic objectives and planning and its past, present and future research and development), technical, functional and scientific requirements and specifications, data concerning business relationships, demonstrations, processes, machinery, know-how, architectural information, information contained in a party’s software and associated material and documentation, plans, designs and drawings and all material of whatever description, whether subject to or protected by copyright, patent or trademark, registered or un-registered, or otherwise disclosed or communicated before or after the date of this process.
3. The receiving party shall not, during the period of validity of this process, or at any time thereafter, use or disclose, directly or indirectly, the confidential information of SITA or the client (even if received before the date of this process) to any person whether in the employment of the receiving party or not, who does not take part in the performance of this process.
4. The receiving party shall take all such steps as may be reasonably necessary to prevent SITA and the client confidential information coming into the possession of unauthorised third parties. In protecting the receiving party’s confidential information, SITA and the client shall use the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorised use or disclosure of the confidential information as the receiving party uses to protect its own confidential information.
5. Any documentation, software or records relating to confidential information of SITA or the client, which comes into the possession of the receiving party during the period of validity of this process or at any time thereafter or which has so come into its possession before the period of validity of this process:
   1. Shall be deemed to form part of the confidential information of SITA or the client;
   2. Shall be deemed to be the property of SITA or the client;
   3. Shall not be copied, reproduced, published or circulated by the receiving party unless and to the extent that such copying is necessary for the performance of this process and all other processes as contemplated in; and
   4. Shall be surrendered to SITA or the client on demand, and in any event on the termination of the investigations and negotiations, and the receiving party shall not retain any extracts.

# Precedence of documents

* 1. This RFI consists of a number of sections. Where there is a contradiction in terms between the clauses, phrases, words, stipulations or terms and herein referred to generally as stipulations in this RFI and the stipulations in any other document attached hereto, or the RFI submitted hereto, the relevant stipulations in this RFI shall take precedence.
  2. Where this RFI is silent on any matter, the relevant stipulations addressing such matter and which appears in the SITA Procurement Policy and Procedures shall take precedence. RFI shall refrain from incorporating any additional stipulations in its RFI submitted in terms hereof other than in the form of a clearly marked recommendation that SITA may in its sole discretion elect to import or to ignore. Any such inclusion shall not be used for any purpose of interpretation unless it has been so imported or acknowledged by SITA.
  3. It is acknowledged that all stipulations in the SITA Procurement Policy and Procedures are not equally applicable to all matters addressed in this RFI. It however remains the exclusive domain and election of SITA as to which of these stipulations are applicable and to what extent. The bidders are hereby acknowledging that the decision of SITA in this regard is final and binding. The onus to enquire and obtain clarity in this regard rests with the bidders. The bidders shall take care to restrict its enquiries in this regard to the most reasonable interpretations required to ensure the necessary consensus.

# Briefing and information session

* + 1. A Non-compulsory virtual briefing session will be held on 18 November 2022.
    2. Bidders who respond to this RFI may be requested to give an oral presentation.

# Submission of documents

* 1. Bidders shall submit RFI response in accordance with the prescribed manner of submissions as specified below.
  2. RFI responses must be submitted electronically to SITA at [Tenders@sita.co.za](mailto:Tenders@sita.co.za) on or before 11 May 2023 not later than 11h00 South African Standard Time (UTC+2).
  3. Respondents are requested to complete their responses in electronic format, in the spaces provided for answers within this document.
  4. All additions to the information documents i.e. appendices, supporting documentation, photographs, technical specifications and other support documentation covering suggested solutions etc. shall be submitted as part of this RFI. No product information or company profiles will be considered.
  5. No information shall be accepted by SITA if submitted in any manner other than as prescribed above.
  6. SITA will not be liable for any costs incurred by the respondents in the preparation of response to this RFI. The preparation of responses will be made without obligation to accept any of the suggestions included in any response, or to discuss the reasons why such suggestions were accepted or rejected.

# TECHNICAL INFORMATION REQUEST ON SOFTWARE CONFIGURATION MANAGEMENT SOLUTIONS FOR z/OS SOFTWARE DEVELOPMENT

1. In the submission to the Request for Information (RFI) the responded are requested to submit detailed information including costing model and option for the implementation of the SCM Solution for z/OS Development. Detailed information (architecture) for the implementation of the solution must be included with the following requirements:

### Software Configuration Management Requirements

#### Life Cycle management

An SCM solution should provide a fully customisable life cycle for source code artefacts. A typical life cycle could consist of a Development, Test, QA and Production stage. The solution must also provide for an Emergency Maintenance stage that bypasses the normal life cycle for emergency changes.

#### Version Control

Version control is a critical function of SCM. Source code artefacts change over time in a software development or maintenance environment. A complete history of all these changes must be kept. The SCM solution must provide a method of recalling any previous version of any source code artefact. It must also provide a function to compare any two versions of a source code artefact.

#### Access control

Source code artefacts for different systems or projects might have different security classifications. The SCM solution must control this access by means of a robust built-in role-based security layer.

#### Approval and control of software deployments

The SCM solution must allow for the approval of any source code promotion through the life cycle.

#### Automated build of runtime artefacts

An efficient software development or maintenance environment leverages automation to increase productivity and integrity of runtime artefacts. The SCM solution should provide the ability to automate the processes required to create these objects for the runtime environment.

#### Support for all major z/OS software development languages

Due to the fact that the SCM solution will be used across multiple software development and maintenance teams within the DOD, support will be required for all major z/OS software development languages.

#### Management reporting capability and auditing purposes

Management reports are drawn for control of software development and maintenance projects. Reports will also be requested from the system for auditing purposes, specifically with regards to source code changes for a specified time period and project.

#### Operating systems: z/OS

The SCM solution must be hosted on a z/OS platform.

#### Integration with Incident logging system

The SCM solution must be able to integrate with existing Incident Logging systems. The incident numbers (or tickets) will be used to group source code changes and tracked on the SCM throughout the life cycle. Manual entry of incident numbers or tickets is acceptable.

#### Batch interface

The SCM solution must provide a batch interface (i.e. tools that can be invoked from Job Control Language (JCL)) to execute common SCM tasks. Batch interfaces assist greatly with automation.

## Consideration and Constraints

Cognizance should be given to the mandate that SITA must improve service delivery to the public through the provision of information technology, information systems and related services in a maintained information system security environment to the departments and public bodies; and promote the efficiency of departments and public bodies through the use of information technology.

The solution should be able to provide support for:

* Life Cycle management
* Version Control
* Access control to source code artefacts
* Approval and control of software deployments
* Automated build of runtime artefacts
* Integration with deployment tools
* Support for all major z/OS software development languages: COBOL, C, Assembler, REXX, CLIST, JCL
* Management reporting capability and auditing purposes
* Operating systems: z/Linux and Windows Server
* Integration with Incident logging system. Manual entry of incident numbers or tickets is acceptable.
* Batch interface

## Integration Requirements for Software Configuration Management

* The product/tool should:
* be able to integrate with an external call logging or incident logging system. Manual entry of incident numbers or tickets is acceptable.
* be able to minimize Business interruptions
* be able to reduce the costs associated with unplanned application downtime
* be able to increase productivity and efficiency.

|  |  |
| --- | --- |
| Question | Vendor Response |
|  |  |
| Company Name |  |
|  |  |
| Primary Contact Number |  |
|  |  |
| Primary Email Address |  |
|  |  |
| Business Background |  |
|  |  |
| OEM Company Country of Origin |  |
|  |  |
|  |  |
| How does your company define SCM? |  |
|  |  |
| Is your company solution included on Gartner’s Magic Quadrants? |  |
|  |  |
| Are your SCM solutions delivered directly or through a 3rd party in South Africa? |  |
|  |  |
|  |  |
| Is your product fully Windows 10 compatible at the end user interface. |  |
|  |  |
| Does your solution provide a fully customisable lifecycle, including an emergency maintenance stage? |  |
|  |  |
| Does your solution provide full version control of source code artefacts? |  |
|  |  |
| Does your solution provide strict access control to source code artefacts? |  |
|  |  |
| Does your solution include role-based access control per project? |  |
|  |  |
| Does your solution provide approval of software deployments? e.g. to be approved by specific roles. |  |
|  |  |
| Does your solution provide an automated build functionality of runtime artefacts? |  |
|  |  |
| Does your solution provide integration with deployment tools? e.g Make |  |
|  |  |
| Does your solution support all major z/OS software development languages, including but not limited to: COBOL, C, Assembler, REXX, CLIST, JCL? |  |
|  |  |
| Does your solution cater for customization of lifecycles, build tools, automation? |  |
|  |  |
| Does your solution provide a reporting capability for management and auditing purposes? E.g. Changes made in a specific time span etc |  |
|  |  |
| Is your solution supported on a z/Linux or Windows Server Operating System? |  |
|  |  |
| Does your solution provide integration with an external Incident logging system? Manual entry of incident numbers or tickets is acceptable. |  |
|  |  |
| Does your solution provide a batch (JCL) interface to execute common SCM tasks? |  |
|  |  |
| Does your product support all the above in a single product, a suite of products or does it require external products? If so, please elaborate. |  |

### INTEROPERABILITY

The Software Configuration Management Solution for z/OS Development must adhere to the government MIOS. It will be used to scan and identify vulnerabilities from different devices, operating systems, application, database software, etc.

### SPECIAL REQUIREMENTS

SITA requires a proposal that will detail options available to update the vulnerability scanner database. SITA reserves a right to or not request the responders to make presentation of their solutions proposals.

### TRAINING

The Responder must include all details on the training and/or skills transfer availability on the proposed vulnerability management solution.

# Contact details

The following contact details are applicable:

1. For general enquiries contact [Lunathi.Mqalo@sita.co.za](mailto:Lunathi.Mqalo@sita.co.za)
2. For technical enquiries contact [Gerhard.Els@sita.co.za](mailto:Gerhard.Els@sita.co.za)
3. Terms and definitions

# ABBREVIATIONS

ICT Information and Communication Technology

SITA State Information Technology Agency

1. DEFINITIONS

|  |  |
| --- | --- |
| “Must” | Indicates a mandatory action which is subject to verification. |
| “Must not” | Indicates a prohibited action which is subject to verification. |