



RFI NO: SAMSA/RFI-01/2024/25: THE SOUTH AFRICAN MARITIME SAFETY AUTHORITY MARITIME WOULD LIKE TO REQUEST INFORMATION FROM THE CLOUD SERVICE PROVIDERS (CSP) TO DETERMINE THE NUMBER OF SERVICE PROVIDERS AND THEIR SERVICE PORTFOLIO RELATING TO THE PROVISIONING OF CLOUD SERVICES

PART 1

1.1 LETTER OF INVITATION TO THE SERVICE PROVIDER:

SUBMISSION OF RFI RESPONSES:

The Request for Information (RFI) responses must be sealed and delivered at the South African Maritime Safety Authority Office, in the Tender Box located at the following address:

146 Lunnon Road
Cnr Jan Shoba & Lunnon Road
Hillcrest
0183

All submissions responses must be clearly marked as follows:

Attention: Z Sibiya : SCM
zasibiya@samsa.org.za

From : Name of company
Company address
Contact details of company representatives

ISSUE DATE: 18 MARCH 2025

CLOSING DATE: 09 APRIL 2025 at 11:00 am

BRIEFING SESSION - Non-compulsory

VENUE: Virtual via Microsoft Teams

Date: 26 MARCH 2025

TIME: 14H00-15H00

Link – Microsoft Teams

[Join the meeting now](#)

Meeting ID: 357 577 798 054 Passcode: TT99K5BT

Companies responding to the RFI should consider the following important issues:

- No questions, during the RFI period will be answered telephonically.
- All questions must be submitted in writing via the email address:
- No late submission will be accepted
- Sealed and signed by person(s) duly authorized to act on behalf of your company
- Submissions must be received in full

1. INTRODUCTION

1.1. The South African Maritime Safety Authority (SAMSA) was established on the 1st of April 1998 under the SAMSA Act 5 of 1998. The objectives of the Authority are:

- To ensure safety of life and property at sea.
- To prevent and combat pollution from ships in the marine environment; and
- To promote the Republic's maritime interests.

SAMSA has also been charged with the responsibility of executing the following:

Administration of the Merchant shipping (National Small Vessel Safety) Regulation, 2007, as amended (the Regulations). The Regulations extends SAMSA's Core mandate to include inland waterways (only waterways accessible to the public) within the Republic. That is to ensure boating safety on our waters.

- Implementing and executing the Long-Range Identification and Tracking (LRIT) of vessels along the South African coastline. The Long-Range Vessels monitoring system assists in securing South Africa's coastal waters in the midst of the rising lawlessness at sea, with particular reference to the worrying scourge of pirate attacks along the east coast of Africa. SAMSA's head office is based in Pretoria, while there are 8 other offices based along the South African coastline.

To deliver effectively on its mandate, SAMSA has adopted usage of technology to deliver on its mandate. The provisioning of optimal, secure and resilient ICT environment to host ICT services has become critical for the current and future hosting of SAMSA ICT requirements of SAMSA. To enable an environment that can accommodate such requirements, cloud computing is now in the mainstream capable of providing on-demand resources such as computing power, data storage capacity, software and related services.

The National Institute of Standards and Technology (NIST) defined Cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud model is comprised of three service models (Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)) and four deployment cloud models (Private, Community, Public and Hybrid).

2. PURPOSE

The purpose of this document is to Request for Information (RFI) from available Cloud Service Providers (CSP) for SAMSA to understand the Cloud computing services market with a view to get a compressive view of the CSPs market and their services portfolios.

3. OBJECTIVES OF THE REQUEST FOR INFORMATION

To align with the requirements of the Determination and Directive on the usage of Cloud Computing services in the Public Services including the National Policy on Data and Cloud. The cloud computing directive provides that the public service should ensure that the cloud services are a first option to be explored before any on-premises infrastructure investment is committed.

The National Policy on Data and Cloud provides that Government departments and entities shall prioritise cloud services as the primary option for new ICT procurement. As described above, SAMSA intends to publish the RFI to determine the following with regards to the provisioning of cloud services in South Africa by the available CSPs:

- To gather information relating to the available service providers in the market who provides the Cloud services.
- To understand the service provider composition of their service portfolios relating to the provisioning of cloud services.
- To understand the service provider costing structure relating to the provisioning of their cloud services.
- Compliance to related regulations, directives, policies, etc.
- To identifying appropriate suppliers who can respond to an RFP for the provisioning of Cloud Services for SAMSA.

4. SCOPE OF CLOUD SERVICES

In the context of this RFI, cloud services would include all the technologies, services (technical, professional, managed, etc) and related required for effective implementation and management of cloud services. The scope of the RFI would cover the provisioning of services in either of the three service models including either of the deployment models with focus on and not limited to the following:

Service	Description
1. Cloud Service Provider (CSP) Profile	Description of the profile of the CSP, years of cloud experience, service portfolio, areas of operations, etc.
2. Infrastructure	
2.1. Size and reach	Description if the CSP offer services locally or it has a global present. If the CSP offers services in different geographic locations, details relating to provision of services locally should be outlined.
2.2. Compute	Description of the full portfolio of compute services with the outline of available options.
2.3. Networking	The CSP to outline a full description of the network services available as part of the CSP portfolio.
2.4. Database	Description of the full database capabilities within the CSP portfolio including database management services.
2.5. Storage	Description of the full portfolio of services relating to the provisioning and management of storage.
Big Data, Analytics, AI, IOT, etc	Full description of the available services with the CSP portfolio that relates to: ▪ Big data management, ▪ Analytics, ▪ Artificial Intelligence,

	▪ Internet of Things and ▪ Related new digital technologies.
Administration	Description of the provisioning of services relating to effective and secure administration of the CSP cloud environment and services.
Security	Provisioning of a secure and resilient environment is critical for provisioning of ICT services. The CSP is required to provide a clear outline of the available security solutions and services to ensure protection of the following cloud components: ▪ Security of tenant. ▪ Network ▪ Data ▪ Application Programming Interfaces (API). ▪ Access control and User accounts. ▪ Vulnerability Management. ▪ Secure configuration. ▪ Encryption, key management, etc. CSP are encouraged to provide a comprehensive response and include other security components not listed above.
Backup, Archiving and Disaster Recovery	CSP description of the services provided relating to backups, archiving and DR. The response to include the CSP business continuity measures to ensure high availability of services.
Compliance, accreditation and certifications	The CSP to provide compliance relating to and not limited to the following: Certifications: ▪ International Standards Organisation (ISO). ▪ SOC 1 and SOC 2. Legislation, regulations, etc: ▪ Protection of Personal Information Act (POPIA). ▪ DPSA Cloud Determination and Directive. ▪ South African National Data and Cloud Policy. Frameworks: ▪ CIS ▪ NIST
Professional Services	Description of the full bouquet of technical and consulting professional services available to support the customer to fully migrate and operate the workloads/services hosted on the CSP cloud environment including training.
Support and maintenance	The CSP to provide full description of how they support they support and maintenance the provisioned cloud services. The response to provide the full scope of the available support and maintenance services
Costing	The CSP to provide the costing structure of all billable

	services that form part of the cloud services across. The costing structure is critical to determine issues of budgeting and costs control.
Contracting and Service Level Agreements (SLA)	Description of the CSP contracting models including the services level such as: ▪ Service hours 24/7x365. ▪ Service availability 99.95%. The CSP to provide details relating to the requirements when exiting the CSP to another.

5. RESPONSE SHEET FOR THE REQUEST FOR INFORMATION

The CSP responding to this RFI are encouraged to be as description and comprehensive as possible and not limit the responses to the services described above. This will enable SAMSA to achieve the objective of publishing the RFI which is aimed to understanding fully the CSP market size and the available services.

6. ASSESSMENT CRITERIA

6.1 SAMSA will follow a three-phase process as follows

- Phase 1: Assessment of the information provided.
- Phase 2: Assessment of the cost breakdowns provided.
- Phase 3: Compiles Terms of Reference and embarks on the appropriate SCM process.

6.1.1. Phase 1: Assessment of the information provided

Compliance with Requirements

Criteria: Evaluate whether the information meets all the requirements outlined in the request for Information (RFI) as described in section 4 above.

6.1.2 Phase 2: Cost breakdown

Bidder to provide cost breakdown

6.1.3 Phase 3: SAMSA Compiles Terms of Reference and Embarks on the appropriate SCM Process

SAMSA will embark on the appropriate SCM process following the completion of Phase 1 and 2.

SAMSA reserves the right to combine proposed solutions for compiling the Terms of Reference (**TOR**), which will be advertised by means of an appropriate SCM process.

7. SUBMISSION OF RFI RESPONSES:

As described above, the CSP are required to submit one original of the responses together with a digital version in a USB/memory stick, in sealed envelope clearly marked RFI Response – **SAMSA/RFI-01/2024/25: REQUEST FOR INFORMATION FROM THE CLOUD SERVICE PROVIDERS (CSP) TO DETERMINE THE NUMBER OF SERVICE PROVIDERS AND THEIR SERVICE PORTFOLIO RELATING TO THE PROVISIONING OF CLOUD SERVICES** and should be deposited in the box located at the reception.

Physical Address

South African Maritime Safety Authority
146 Lunnon Road
Cnr Jan Shoba & Lunnon Road
Hillcrest
0183

The RFI number and the description **MUST** be clearly indicated on the cover of the bid document. It is the responsibility of each service provider when submitting to ensure that they complete the RFI Register at the Reception. The closing date and time for receipt of responses is **09 APRIL 2025** at 11H00.

IT IS THE RESPONSIBILITY OF EACH SERVICE PROVIDER TO ARRIVE EARLY TO SUBMIT THE RFI RESPONSE DOCUMENTS AS THEY WILL BE REQUIRED TO FOLLOW BUILDING SECURITY PROTOCOLS OF REGISTRATION. SAMSA WILL NOT BE RESPONSIBLE FOR BIDDERS WHO ARRIVE LATE AND CLAIM THAT THEY WERE HELD AT SECURITY FOR REGISTRATION, WHICH WILL NOT BE ACCEPTED AS A REASON FOR LATE ARRIVAL OR LATE SUBMISSION.

7. RFI RELATED ENQUERIES

All SCM and technical related enquires should be directed to:

- Zanele Sibiyi on 012 366 2600 or zasibiyi@samsa.org.za