4th Meeting of the SIOFA VMS Working Group (VMSWG-02)

Online, 22 November 2024

VMSWG-04-01

Options Paper for the Hosting of the SIOFA Vessel Monitoring System

SIOFA Secretariat

Document Type	working paper ✔ information paper ☐
Distribution	Public ✔ Restricted [1] ☐ Closed session document [2] ☐

Abstract

Following the adoption of CMM 16 (2023) and the SIOFA VMS SSPs, the VMS WG was tasked to inform the MoP of potential hosting options for the SIOFA VMS, highlighting the potential resource implications of these options for its consideration and to provide the necessary recommendations to this end. This paper sets out two possible hosting options: an onsite option (Software as a Product (SaaP)) and a remote/cloud-hosted option (Software as a Service (SaaS)) and aims to:

- explain the two options;
- provide an overview of the VMS systems implemented in other RFMO/Bs and CCAMLR; and;
- to set out the resource and cost implications of the proposed options for SIOFA.

Rev1 of the annexed Options paper includes an amendment to the original paper circulated via Circular No. 2024-32, which is to include a "contingencies" line in the 5-year Op-Ex projections (Tables 3 and 4).

Recommendations (for proposals and working papers only)

- That the SIOFA VMS WG notes and considers these hosting options and makes a recommendation to the CC/ MoP on a preferred hosting option for the SIOFA VMS

[1] Restricted documents may contain confidential information. Please do not distribute restricted documents in any form without the explicit permission of the SIOFA Secretariat and the data owner(s)/provider(s).
[2] Documents available only to members invited to closed sessions.

Options Paper for the Hosting of the SIOFA Vessel Monitoring System

Rev1

VMS WG Chair and SIOFA Secretariat

SIOFA | APSOI

Southern Indian Ocean Fisheries Agreement

Accord relatif aux Pêches dans le Sud de l'Océan Indien

Southern Indian Ocean Fisheries Agreement (SIOFA)
13 Rue de Marseille
97420 Le Port
La Réunion

secretariat@siofa.org
www.siofa.org

Table of Contents

1. Introduction

The 10th Meeting of the Parties (MoP10) for the Southern Indian Ocean Fisheries Agreement (SIOFA) adopted a Conservation and Management Measure to Establish a SIOFA Vessel Monitoring System (SIOFA VMS).[1] The MoP10 also established an intersessional working group (VMS WG) to support the entry into operation of the SIOFA VMS. Some of the work completed by the VMS WG includes the Standard, Specifications and Procedures for the SIOFA VMS (VMS SSPs), which was formally adopted by the 11th Meeting of the Parties (MoP11) and a Roadmap towards the establishment of the SIOFA VMS.

Following this, the VMS WG was tasked to inform the MoP of potential hosting options for the SIOFA VMS, to indicate the potential resource implications of these options for its consideration and to provide the necessary recommendations to this end. This should provide the MoP with an understanding of the various hosting options for the SIOFA VMS and their potential resource implications, including staffing, financial resources, and other infrastructure considerations for operationalizing the SIOFA VMS.

The MoP should have, through this paper and the work of the VMS WG, a broad understanding of how the operationalization of the SIOFA VMS can be expected to impact SIOFA policies and the SIOFA budget, including capital costs and operational expenses, recalling that CMM 16 (2023) foresees that the Secretariat will administer the SIOFA VMS.

To better understand these modalities and their implications, the Secretariat examined VMS systems implemented by other Regional Fisheries Management Organizations (RFMOs), Regional Fisheries Bodies (RFBs), and the Commission for the Conservation of Antarctic Marine Living Resources (CCAMLR).

The Secretariat also engaged with some service providers to get a better understanding of the potential indicative costs of establishing a SIOFA VMS including recurrent direct costs.

On this basis, this paper sets out two possible hosting options: an onsite option (Software as a Product (SaaP)) and a remote/cloud-hosted option (Software as a Service (SaaS)) and aims to:

- explain the two options;
- provide an overview of the VMS systems implemented in other RFMO/Bs and CCAMLR; and;
- to set out the resource and cost implications of the proposed options.

[1] Conservation and Management Measure for the establishment of a SIOFA Vessel Monitoring System (CMM 16 (2023) (Vessel Monitoring System).

2. General Information

There are 103 vessels currently on the SIOFA Record of Authorized Vessels (RAV)[2] flagged to the 13 SIOFA CCPs. These vessels spend around 10,000 days per year in the Area.[3]

Currently, CMM 10 (2023) (Monitoring)[4] requires CCPs to implement domestic VMS programs which comply with SIOFA minimum standards, but does not require CCPs to share VMS position reports with the Secretariat. This set-up has no implications for the SIOFA budget, as the related costs are limited to those associated with CCPs' domestic VMS programs.[5]

When the SIOFA VMS becomes operational, these vessels will be required to transmit VMS position reports to the SIOFA VMS while operating in the Agreement Area. CCPs will have the option to require their vessels to send VMS position reports simultaneously to the Secretariat via their Fisheries Monitoring Center (FMCs) (CMM 16 (2023), paragraph 6.a), or simultaneously to both the Secretariat and their FMC (paragraph 6.b). Between these two options for transmitting VMS position reports, the option provided by paragraph 6. b) may have higher cost implications for CCPs compared to paragraph 6. a) as service providers typically charge additional fees to send duplicated VMS position reports to a third party, which in this case will be the SIOFA Secretariat, while forwarding them via an FMC come at no cost to the CCP.

Under CMM 10 (2023), CCPs are currently required to ensure that their vessels flying their flag report VMS position reports automatically while in the Area vessel at least once every hour when vessels fishing for *Dissostichus* spp. are in the Del Cano Rise area, and at least once every two hours in other circumstances. These reporting frequencies will not change when the SIOFA VMS enters into operation.

All vessels currently registered on the SIOFA RAV carry an Automatic Location Communicator (ALC) on board as required by CMM 10 (2023).[6] Based on the information available on the SIOFA RAV, most of the ALCs deployed on board these vessels already meet the requirements of CMM 16 (2023), including its Annex 1, and the SIOFA VMS SSPs. As such, it is not expected that there would be any need to deploy new ALCs on board vessels.

The ALCs currently deployed on board authorized vessels use a range of brands and service providers to transmit data to their flag FMCs, with *Collecte Localisation Satellites* (CLS) being the most dominant brand by a large margin. Other brands include Cobham/ Sailor, Thrane and Thrane, Furuno, and Satlink (Figure 1). Data transmitted by these ALCs are transmitted over three main satellite networks: Argos, Iridium, and Inmarsat (Figure 2), with Iridium being the most widely used satellite network.

[2] October 2024.
[3] Based on 2022 and 2023 entry / exit reports submitted to the Secretariat.
[4] Conservation and Management Measure for the Monitoring of Fisheries in the Agreement Area (CMM 10 (2023) (Monitoring).
[5] With the understanding that some CCPs may be party to other RFMOs and/or RFBs that require transmission of VMS position report to a regional VMS, and therefore may have financial implications in this regard.
[6] Based on information submitted by CCPs when notifying the Secretariat of vessels authorized to operate in the Area, and to be entered onto the SIOFA RAV, and other sources such as Port Inspection Reports (PIR).

Considering the data standards set out in the VMS SSPs for the transmission of VMS position , it is also expected that CCPs will not need to adapt their current VMS systems to enable the transmission of VMS position reports to the SIOFA VMS.

Figure 1. ALC Brands Currently Deployed on Authorized Vessels

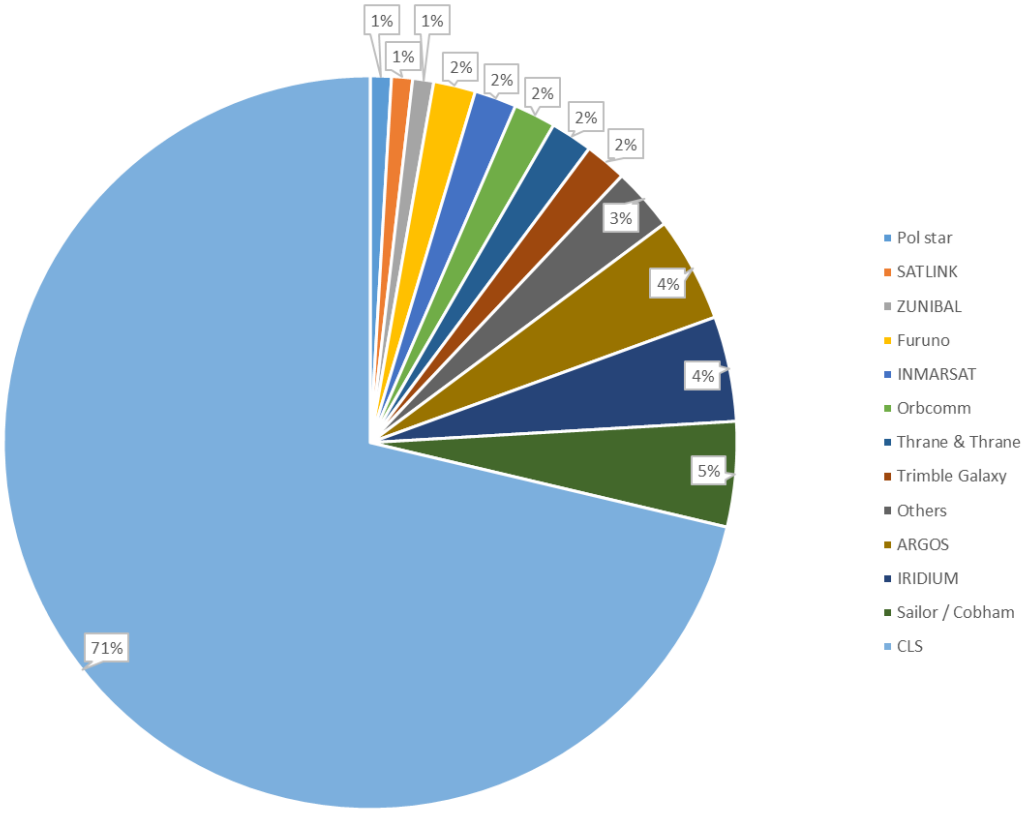
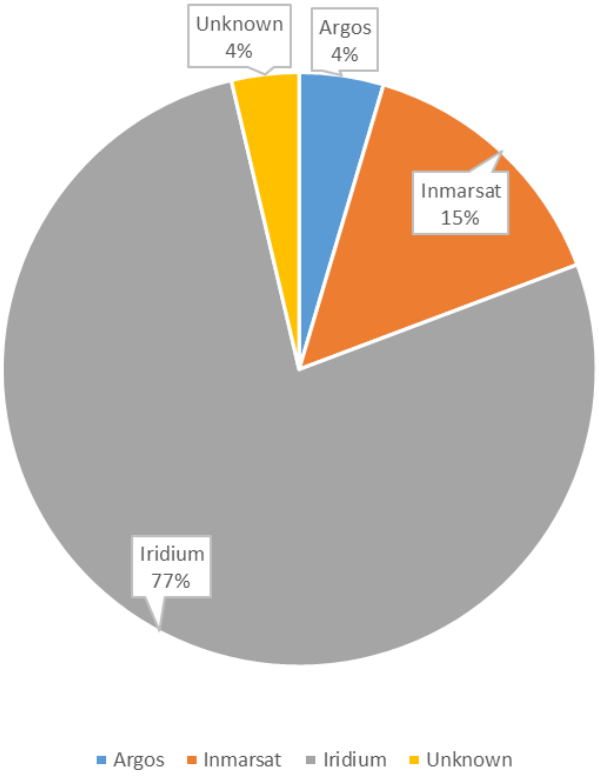


Figure 2. Sattelite Service Provider Used by ALCs Deployed on Authorized Vessels



3. Hosting Options for the SIOFA VMS

To allow the Secretariat to receive VMS position reports, SIOFA will need to acquire a specialized VMS application that will enable it to receive, process, visualize, and retransmit VMS position reports. As identified by the VMS WG, one of the decisions required by the MoP is whether to host the SIOFA VMS within or outside the Secretariat. In other words, the MoP needs to decide on the "software (VMS Application) delivery model" for the SIOFA VMS.

In most applications similar to what is envisaged for the SIOFA VMS, there are two common software delivery models (referred to as "hosting options" in SIOFA policy documents and reports) to deploy and operationalize the service required by the client and end users. These are *Software as a Product* (SaaP) or on-premise deployment solutions, and *Software as a Service* (SaaS) primarily referring to remote or cloud solutions.

Implementation of both delivery models varies from application to application, but in general, both options offer varying levels of benefits in terms of costs, infrastructure requirements, resource needs, and security. In both cases, the client's needs can be accommodated to the extent permissible by these respective technologies.

Both delivery models are capable of meeting the requirements of SIOFA CMMs, notably CMM 03 (2016) (Data Confidentiality),[7] CMM 16 (2023) and the SIOFA VMS SSPs.

This section aims to provide an understanding of these two delivery models by providing an overview and comparison of the models' general attributes and highlighting their advantages and disadvantages in relation to the SIOFA VMS.

3.1 Software as a Product (SaaP)

SaaP is software designed to be sold to users who pay for a license that allows them to deploy, host, install, and use it on the client's infrastructures, such as internal data centers, servers, and personal devices. Applications similar to the SIOFA VMS entail an IT infrastructure where all hardware, software, and data storage are managed onsite, and the client (which in this case would be SIOFA) maintains all processes associated with the application.

Most SaaP solutions offer a one-off payment structure. However, it is typical with VMS applications that the purchase will also include long-term maintenance contracts that will result in considerable recurring costs. This is in view that VMS applications usually require regular maintenance to ensure maximum uptime and reduce disruptions, especially in medium to critically demanding environments. Changing standards and governance requirements related to regional fisheries management may also require regular updating of the solution at a cost. Typical service contracts also include these updates to the SaaP solutions in VMS applications.

3.2 Software as a Service (SaaS)

Software as a service (SaaS) is a form of cloud computing in which the provider offers the use of application software to a client and manages all the physical and software resources used by the application. The distinguishing feature of SaaS compared to SaaP is that it separates the possession and ownership of software from its use. SaaS are usually subscription-based solutions. Typical SaaS providers are responsible for providing data security, server availability,

[7] Conservation and Management Measure for Data Confidentiality and Procedures for access and use of data.

and the agreed-upon performance standards. Therefore, it comes with no high upfront cost for the client or organization and requires minimum infrastructure investments and modifications to join the service. The organization will only need to invest in an adequate internet connection and modify or upgrade the workstations if needed to access the service.

It is observed in many instances that SaaS applications offer as much, if not more, functionality than their SaaP counterparts. SaaS also reduces deployment time as there is no need to ship hardware associated with the service, and no installation and onsite configuration is required to start utilizing the service.

3.3 General Attributes of the Delivery Models

3.3.1 Deployment Location

SaaP solutions are located within an organization's IT infrastructure and domain. They use the organization's resources, space, and utilities to function, and as such, the organization must accommodate and maintain all processes associated with this solution. This is a crucial element to consider as SaaP generally requires more "in-house" resources compared to SaaS solutions. In the case of SIOFA, the necessary space has been identified within the Secretariat to host the servers and infrastructures associated with a SaaP VMS solution. However, the space will need to be retrofitted with the necessary equipment to accommodate the server cluster. This should include redundant power supplies for 24-hour uptime, air conditioning and dehumidifiers to regulate humidity and temperature, server racks and accessories.

Long-term maintenance of the equipment, including the servers, needs to be factored in when planning the operational costs of the SIOFA budget associated with the SIOFA VMS. Equipment running 24 hours a day, 7 days a week, also requires a rigorous maintenance schedule, with equipment requiring replacement on average every five years. This will ensure minimum downtime and efficient operation of the SIOFA VMS over time. As such, it should be noted that with SaaP, the cost of setting up the infrastructure to support the SIOFA VMS may be significant, both in terms of capital investments and operational costs.

SaaS, on the other hand, is hosted outside of the organization, as mentioned above. This is usually on remote servers or cloud infrastructures in the form of *Infrastructure as a Service*. As the provider is responsible for the resources associated with providing the service, the clients and organization do not have to make physical space available for those, nor do they have to deploy new infrastructure to subscribe to and access the service.

All of those are included in the subscription plan for accessing the application (VMS). Consequently, SIOFA would not have to cater for financial or human resources to deploy and maintain any server and equipment associated with the application. The maintenance budget for the VMS would be limited to the workstations used by the staff to access the service and the infrastructures required to access the VMS, which should be significantly less than the maintenance resources required for a SaaP VMS solution.

SaaS applications are accessed via the internet, so the quality of service will depend on a stable internet connection. Internet connectivity or third-party issues do not hinder access to SaaP services, although the Internet is still required to receive VMS position reports.

3.3.2 Control

SaaP solutions offer more control over the system, its features and the operating environment. In most cases, organizations or clients manage their servers and software configuration and customization based on internal policies and specific services required. However, the gap between SaaP and SaaS has been closing in recent times, with SaaS providers offering more and more customizability when it comes to control, allowing organizations to customize the solutions based on their needs.

One drawback of SaaP solutions in this regard is that while they offer more control, these do come at a cost, especially if the customization requires new development by the supplier or needs additional infrastructure.

While SaaS is regarded as inferior in terms of control, newer SaaS are offering solutions close to, or on par with, their SaaP counterparts. Often, the implementation of the control relies on the service provider, and may be limited by the hosting technology being used by it.

3.3.3 Security

SaaP arguably provides more robust security than its counterpart SaaS, but recent trends show that the gaps between the two are quickly narrowing, with SaaS providing increasingly robust security solutions, in some cases on a par with current SaaP applications. However, the level of security of SaaP applications is contingent on the robustness of the organization's infrastructure and, therefore, will have a direct impact on how secure the system would be, as the client or organization is responsible to implement security measures within its infrastructure, either in-house or outsourced to specialized IT security companies. The downside is that implementing robust security measures may require significant investment and long-term maintenance costs. The system's location within the organization adds another layer of security, although this is also contingent on the infrastructure's robustness.

Improvements in security in SaaS application for the duration of the service will not require any significant investments other than those to be implemented by the Secretariat. Furthermore, all security requirements can also be included in service-level agreements to ensure that the provider is contractually required to provide those as part of the service.

3.3.4 Scalability

The scalability of a SaaP application is not as flexible as its counterpart, SaaS. In the SIOFA context, this means that once the system is deployed to accommodate current and forecasted data flow, any significant increases in data flow, which may come as a result of policy decisions (e.g. to implement an Electronic Reporting System for catch and effort reporting, or less dramatic changes such as increase in reporting frequency) may require substantial reinvestment in the system including new hardware and infrastructure to accommodate the increased demand.

SaaS deployments are far more flexible in this regard, as resources are dynamically allocated by the provider based on traffic and services required by the client. Therefore, SaaS should be able to accommodate any significant changes in demand by SIOFA, with the only consequence being the potential increase in subscription costs. This also makes SaaS applications future-proof, providing reassurance of their long-term viability.

3.3.5 Cost Structure and Expenses

The typical cost structures of SaaP applications are one-off costs, which, in the case of a VMS system, usually include the associated hardware (servers mostly). However, because of the nature of the VMS system, such acquisition also includes support and maintenance contracts that ensure that the system, including both hardware and software, is well supported throughout its life cycle. Support and maintenance contracts includes support in the event of critical system failures. They are usually renewable on an annual basis but could also be longer depending on the negotiated terms.

As SaaS is subscription-based (usually annually), upfront costs are minimal and, in most cases, non-existent. The costs usually reflect the service being provided and are not contingent on the amount of data the client receives. However, the cost of the services consulted may be impacted by the number of vessels the client monitors. Further, with SaaS systems, the maintenance cost of the system is included in the service cost as the provider is responsible for it.

3.3.6 Upgrades and Maintenance

As VMS becomes more demanding, features are added to keep up with developments in regional and global fisheries governance requirements, necessitating regular software upgrades and deployment so FMCs globally can effectively monitor fishing and related activities. As such, these applications require regular software updates to keep up with those developments so that these new tools can serve the purposes of FMCs globally (e.g., using Artificial Intelligence to assess fishing patterns, automatic data correlation, and risk assessment). Regular hardware and software maintenance is also necessary to ensure optimum system performance and prevent unscheduled downtime due to breakdowns. Given the high availability requirement of the VMS applications, servers and infrastructure are expected to experience higher-than-usual wear throughout their life cycle, usually requiring complete replacement every five years.

In typical SaaP applications, these upgrades require on-site intervention (in some cases, it can be done remotely but with the support of on-site personnel). Upgrades may also require the deployment of new hardware to increase the system's capacity to provide the new services and replace out-of-service hardware due to breakdowns or end-of-life. As such, SaaP applications may require considerable financial and human resources to keep up to date. Further, as SaaP relies more on infrastructure, their regular maintenance and replacement must also be taken into consideration. Therefore, the necessary resources and budget should be allocated.

Upgrades of SaaS applications are done "over the air," meaning that the provider carries out these upgrades on their end without the need for any intervention or support from the client. They become available as soon as the upgrades are deployed, making new features available immediately and in real-time. This is also the case for any additional services that may be required by SIOFA in the future, as indicated above in cases where upscaling is required.[8] These upgrades will require little to no on-site intervention.

In both cases (SaaS and SaaP), maintenance and upgrades will have to consider infrastructure and allocate resources as necessary. As infrastructure requirements differ between the two delivery models, the related cost of infrastructure maintenance for SaaS applications is expected to be much less compared to SaaP applications.

[8] See Section 3.3.4 on "*scalability*".

3.3.7 Data Loss and Redundancies

In systems deployment, data loss refers to unauthorized access to, sharing, downloading, or disclosure of sensitive data stored in a SaaP or SaaS application. Data redundancy, on the other hand, is providing data safety and availability through multiple copies of data on different storage systems against hardware failure, data corruption, or system crashes to ensure data integrity.

While both deployment models allow the client to implement data loss prevention (DLP) measures and ensure data redundancy, SaaP will require suitable infrastructure and technical expertise to fulfil those requirements, typically not provided by VMS service providers. Furthermore, specialized hardware or services will be required to ensure adequate data redundancy.

In contrast, all DLP and redundancies can be included in service-level agreements for SaaS deployments, with data redundancies being an inherent attribute of SaaS deployments.

Table 1 below highlights some of the other direct costs associated with the two systems and how they differ between the delivery models.

Table 1 - Comparison of the various costs associated with SaaP and SaaS Deployment Models

Expense	**SaaP**	**SaaS**
Upfront Cost	Requires significant upfront investment in hardware and infrastructure.	Typically operates on a subscription-based pricing model. It requires less upfront investment.
Maintenance Cost	Requires continuous maintenance resources. It includes space, power, and expert staff.	The service provider maintains the software. It reduces the need for internal maintenance resources.
Scalability Cost	Additional hardware and setup may be necessary for growth, leading to extra costs.	Cloud is scalable with the ability to adapt quickly. Changing business needs without significant additional costs.
Upgrade Cost	Upgrades can be costly as they may require new hardware or system re-configurations.	Software updates are typically included in the subscription cost. These are performed automatically by the provider.
Data Loss Cost	Potential for permanent data loss in case of system malfunctions. Cyberattacks can lead to financial losses.	More robust data protection measures reduce the risk and cost of potential data loss.

Section 5 provides a quantitative and detailed assessment of the potential cost implications of both deployment models.

4. Practices by Other Regional Fisheries Management Organizations / Bodies

4.1 Commission for the Conservation of Antarctic Marine Living Resources (CCAMLR)

Conservation Measure10-04 (2022) Automated satellite-linked Vessel Monitoring Systems (VMS) of the CCAMLR establishes a VMS scheme where vessels are required to report VMS position reports at least once every hour while they are within the "*Convention Area*". It also establishes that these reports shall be sent to the Secretariat, either forwarded by their FMCs or transmitted by their fishing vessels once they are in the Convention Area.

The CCAMLR Secretariat hosts its VMS system on-premise (SaaP). While this approach provides the CCAMLR Secretariat with direct control and security, it does require a significant amount of time from their staff for system management.

Regarding staffing, CCAMLR does not have personnel exclusively dedicated to VMS administration, but compared to SIOFA, they have a sizeable compliance team (4 persons). Managing the system consumes a substantial portion of their staff time. They handle tasks related to system configuration, data analysis, and member support. The Secretariat also provides 24/7 support to members, which presents significant challenges to their team.

The CCAMLR secretariat is also required to provide the necessary infrastructure to support the VMS system as it is a SaaP application. It consumes a significant portion of CCAMLR IT resources, including approximately 25% of processing capacity, 10% of data storage and > 90% of email volume.

The CCAMLR secretariat receives some VMS position reports directly from Inmarsat, which costs approximately AUD$0.05 per VMS position report. On average, this amounts to AUD$12,000 (EUR 7,200) per year. However, most Members retransmit their vessel position reports to the Secretariat via their FMC, and a few use the same VMS service as the Secretariat (CLS), facilitating data sharing at no cost to the Secretariat. The CCAMLR also incurs an annual fee of approximately AUS$ 27,000 (EUR 16,500) for support.

CCAMLR emphasizes the importance of data extraction capabilities for integration with other data sources, data analysis and exploration. This capacity is fundamental for maximizing the utility of VMS data. They believe that it may be time-consuming or even prohibitive to rely only on the provider VMS interfaces for a few analyses relevant to the organization. Additional organisational requirements (e.g., Catch Documentation Schemes, Search and Rescue…) may also require developing separate systems. Some GIS expertise is required for the spatial management of areas and data.

4.2 Other Organizations

The ***North Pacific Fisheries Commission*** (NPFC) VMS became operational in August 2021. They are using a secure cloud solution to store and process the VMS data. NPFC considers this a cost-effective way to manage and analyze the data securely with minimum human capacity. There are five staff members at the secretariat, with one permanent staff member engaged in the day-to-day management of the VMS system and one staff seconded from the host country assisting the compliance department with the VMS system and other compliance services. The data coordinator assists with some of the technical issues related to the VMS. The Secretariat does

not provide 24/7 service to Members, as they have their own domestic system with separate support to assist them.

The data feed is transmitted from the vessel to the flag FMC which then forwards the information for use by NPFC via the VMS contractor. VMS position reports are available to authorized staff in the secretariat.[9] VMS data is provided to Members with enforcement presence in the Convention Area, and is also used during compliance assessments. Members do not retain access to the VMS data after the conclusion of their patrol other than if an investigation is underway.

The Commission VMS of the ***South Pacific Regional Fisheries Management Organisation*** (SPRFMO) was considered fully operational upon its official acceptance by the Commission as of 8 June 2018. Within the SPRFMO Secretariat, the primary oversight of the VMS programme rests with the Compliance Manager (with data support from the Data Manager and invoicing/payment support from the finance officer).[10] VMS issues are the biggest day-to-day tasks of the Compliance Manager, as the system requires oversight and response to alerts and operational issues, which takes time, with around 800 vessels reporting to the commission VMS. Starting the VMS required additional time to work out the bugs and glitches and establish staff training.

CLS, the Commission VMS service provider, manages the software/services/database on their behalf, and the Secretariat uses a secure web interface to view/track/extract data. The SPRFMO is currently building an API to download all the VMS data in THEMIS (the software that is the basis of the Fisheries Monitoring/Management platform) so it is easier to manage for analysis and cross-referencing with other datasets within the Secretariat.

The cost of setting up the SPRFMO Commission VMS, its annual subscription, and staff training is similar to those estimated for the SIOFA VMS. However, for confidentiality reasons, this information is not disclosed in this document.

[9] Compliance Manager, the secondee, the Data Coordinator and the Executive Secretary.
[10] Based on publicly available information, the SPRFMO currently employs five staff in total.

5. Potential Resource Implications of the Options

CMM 16 (2023) provides that the Secretariat will administer the SIOFA VMS. As such, the Secretariat will receive, collate, store, and disseminate VMS position reports, a wholly new function within the Secretariat. It is noted that currently, there exists technical capacity within the Secretariat to handle these VMS position reports.[11] However, resource requirements for administering the SIOFA VMS will differ depending on the delivery model chosen by the MoP, including support for ensuring basic system support.

5.1 System Acquisition

The SIOFA Secretariat will need to procure (or subscribe to) a VMS system to be able to discharge its functions required by CMM 16 (2023). The procurement of a SaaP VMS will include the procurement of the software license, procurement and pre-configuration of servers (around four dedicated servers for the various system modules), shipping, installation and deployment of the system on-site.

SIOFA has been awarded an EU grant for procuring, or the initial subscription to, the VMS system. The grant should be sufficient to either support the partial funding of the procurement of the VMS software and hardware in case the SIOFA chooses the SaaP route or to support the subscription for a few years should it decide to go with a SaaS subscription.

5.2 Infrastructure

The necessary infrastructure for the VMS will vary depending on the deployment model. As indicated previously, a SaaP deployment will require more infrastructure, including a dedicated server room fitted with proper environment controls (air conditioning, dehumidifier), physical access control systems, uninterruptible power supply (UPS), and a suitable network.

A stable internet connection is also needed to receive VMS position reports. The SaaP deployment is also expected to increase the power use of the Secretariat, having a system and supporting infrastructure that will be running 24/7. These will not be a requirement for a SaaS deployment, which would only require a stable internet connection to access the service.

While the EU grant will support the initial purchase and installation of these equipment, its long-term maintenance and regular replacement will need to be supported by the SIOFA Budget.

5.3 Staffing

While the handling VMS position reports and maintaining the SIOFA VMS system will be new functions within the Secretariat, these tasks will be carried out by the Compliance Officer, who has experience with the handling and analysis of VMS data. The feasibility of this arrangement is based on the current workload and expected volume of VMS position reports from fishing vessels, based on approximately 10,000 cumulative days spent in the Agreement Area by the 103 authorized vessels (with some automation within the VMS software). Irrespective of the deployment model adopted by the MoP, this assessment would need to be reviewed if there is a substantial increase in the number of vessels in the coming years, or if MoP policy decisions require the roll-out of additional features (e.g. electronic catch reporting).

[11] Current Compliance Officer's background includes handling and analysis of VMS data.

The Secretariat may need specialized IT capacity to provide the necessary support for the infrastructure. These services may be outsourced on an as-needed basis to private companies. Support to the infrastructure may not be as demanding or require a permanent presence in the case of a SaaS deployment. The need for the permanent support of an IT officer will be compulsory should the SIOFA opt to choose a SaaP VMS application because an on-site presence is necessary to provide technical support such as trouble shooting, data base repairs, etc. As indicated above, SaaP deployment consists of dedicated hardware and a higher level of infrastructure.

Moreover, some additional infrastructures associated with the VMS (Air Conditioning, UPS, and network infrastructure) may require specialized servicing from time to time based on maintenance schedules and when repairs, upgrades or replacements are required. This may, therefore, require the soliciting of outsourced services for those.

The EU support grant foresees building the necessary technical capacity of relevant SIOFA staff to manage and handle VMS data and provide basic IT support to a SaaP deployment.

5.4 Indicative cost

Based on the abovementioned considerations, Table 2 outlines the indicative Capital Expenditure (CaPex) for the procurement and entry into operation of the SIOFA VMS. Tables 3 and 4 outline the indicative Operational Costs (OpEx), projected over five years (n+5) for SaaP and SaaS deployments, respectively.

The OpEx for SaaP includes the cost of replacing hardware after five years of operation, which is their typical lifespan. The OpEx for SaaS is based on registering and monitoring up to 200 vessels.

It should be noted that upscaling and data recovery costs are not provided as they will be unique based on the nature of the upscaling and data loss. Utility and other overheads (except for staffing expenses) are also not included in this assessment; however, as mentioned above, a SaaP deployment will significantly impact overheads, notably the power required to run a 24/7 VMS and Data Centre which will increase the Secretariat's utility costs. It is expected that the amount of received data will not impact subscription costs for a SaaS VMS application(provided there is not drastic changes in registered vessels).

Except for the annual internet subscription cost, all costs below should be considered as surplus to the current SIOFA budget.

In accordance with the SIOFA VMS SSPs, it is not expected that the Secretariat will incur any costs associated with airtime costs or the replacement of ALCs on board vessels if necessary. These costs are to be covered by CCPs for their vessels.

Table 2 - Indicative Capital Expenditures (CapEx), euro

Expense Categories	***SaaP***	***SaaS***	***Notes***
1. System Acquisition	€ 273,900.20	€ 100,886.73	
1.1. System Procurement / Subscription	€ 273,900.20	€ 63,910.20	EU grant
1.2. System Deployment		€ 27,390.00	
1.3. Technical Support		€ 9,586.53	
2. Infrastructure	€ 42,400.00	€ 10,000.00	
2.1. Networking	€ 8,500.00	€ 0.00	EU grant
2.2. Accessories for Servers	€ 1,900.00	€ 0.00	
2.3. Room Temp/ Humidity Control	€ 5,000.00	€ 0.00	
2.4. Server Room and Secretariat Security Improvements	€ 10,000.00	€ 6,000.00	
2.5. UPS	€ 13,000.00	€ 0.00	
2.6. Workstations	€ 4,000.00	€ 4,000.00	
Indicative CapEx	€ 316,300.20	€ 110,886.73	

Table 3 - Indicative Operational Expenditures (OpEx) for a SaaP deployment, euro

Expense Categories	YR-1	YR-2	YR-3	YR-4	YR-5	***Cumulative***
1. System Maintenance	€ 41,085.03	€ 42,440.84	€ 43,841.38	€ 45,288.15	€ 96,884.53	**€ 269,539.93**
1.1 Subscription Fees (Annual)	€ 0.00	€ 0.00	€ 0.00	€ 0.00	€ 0.00	**€ 0.00**
1.2 Hardware Maintenance / Replacement	€ 0.00	€ 0.00	€ 0.00	€ 0.00	€ 50,101.87	**€ 50,101.87**
1.3 Technical Support Contract (Annual)	€ 41,085.03	€ 42,440.84	€ 43,841.38	€ 45,288.15	€ 46,782.66	**€ 219,438.06**
2. Staffing	€ 42,496.26	€ 43,898.64	€ 45,347.29	€ 46,843.75	€ 48,389.60	**€ 226,975.55**
2.1. IT Officer	€ 36,496.26	€ 37,700.64	€ 38,944.76	€ 40,229.94	€ 41,557.52	**€ 194,929.12**
2.2. Staff Capacity Building	€ 6,000.00	€ 6,198.00	€ 6,402.53	€ 6,613.82	€ 6,832.07	**€ 32,046.43**
3. Infrastructure	€ 8,400.00	€ 8,677.20	€ 8,963.55	€ 9,259.34	€ 44,863.95	**€ 80,164.04**
3.1. Internet Subscription	€ 1,000.00	€ 1,033.00	€ 1,067.09	€ 1,102.30	€ 1,138.68	**€ 5,341.07**
3.2. Networking	€ 1,000.00	€ 1,033.00	€ 1,067.09	€ 1,102.30	€ 9,678.77	**€ 13,881.16**
3.3. Accessories for Servers	€ 1,962.70	€ 2,027.47	€ 2,094.38	€ 2,163.49	€ 2,234.89	**€ 10,482.92**
3.4. Room Temp/ Humidity Control	€ 1,500.00	€ 1,549.50	€ 1,600.63	€ 1,653.45	€ 5,693.39	**€ 11,996.98**
3.5. Server Room and Secretariat Security Improvements	€ 2,000.00	€ 2,066.00	€ 2,134.18	€ 2,204.61	€ 11,386.79	**€ 19,791.57**
3.6. UPS	€ 1,000.00	€ 1,033.00	€ 1,067.09	€ 1,102.30	€ 14,802.83	**€ 19,005.22**
3.7 Workstations	€ 0.00	€ 4,132.00	€ 0.00	€ 4,409.21	€ 0.00	**€ 8,541.21**
4. Contingencies (@ 1.1%)	€ 1,012.48	€ 1,045.90	€ 1,080.41	€ 1,116.06	€ 2,092.30	**€ 6,347.16**
5. Annual Inflation Rate	**3.3%**	**3.3%**	**3.3%**	**3.3%**	**3.3%**	**-**
Annual Indicative OpEx	€ 93,056.48	€ 96,127.34	€ 99,299.54	€ 102,576.43	€ 192,301.78	**€ 583,361.56**

Table 4 - Indicative Operational Expenditures (OpEx) for a SaaS deployment, euro

Expense Categories	YR-1	YR-2	YR-3	YR-4	YR-5	***Cumulative***
1. System Maintenance	€ 75,922.12	€ 78,427.55	€ 81,015.66	€ 83,689.18	€ 86,450.92	**€ 405,505.43**
1.1 Subscription Fees (Annual)	€ 66,019.24	€ 68,197.87	€ 70,448.40	€ 72,773.20	€ 75,174.71	**€ 352,613.42**
1.2 Hardware Maintenance / Replacement	€ 0.00	€ 0.00	€ 0.00	€ 0.00	€ 0.00	**€ 0.00**
1.3 Technical Support Contract (Annual)	€ 9,902.89	€ 10,229.68	€ 10,567.26	€ 10,915.98	€ 11,276.21	**€ 52,892.01**
2. Staffing	€ 3,000.00	€ 3,099.00	€ 3,201.27	€ 3,306.91	€ 3,416.04	**€ 16,023.21**
2.1. IT Officer	€ 0.00	€ 0.00	€ 0.00	€ 0.00	€ 0.00	**€ 0.00**
2.2. Staff Capacity Building	€ 3,000.00	€ 3,099.00	€ 3,201.27	€ 3,306.91	€ 3,416.04	**€ 16,023.21**
3. Infrastructure	€ 2,500.00	€ 2,582.50	€ 2,667.72	€ 2,755.76	€ 7,970.75	**€ 18,476.73**
3.1. Internet Subscription	€ 1,000.00	€ 1,033.00	€ 1,067.09	€ 1,102.30	€ 1,138.68	**€ 5,341.07**
3.2. Networking	€ 0.00	€ 0.00	€ 0.00	€ 0.00	€ 0.00	**€ 0.00**
3.3. Accessories for Servers	€ 0.00	€ 0.00	€ 0.00	€ 0.00	€ 0.00	**€ 0.00**
3.4. Room Temp/ Humidity Control	€ 0.00	€ 0.00	€ 0.00	€ 0.00	€ 0.00	**€ 0.00**
3.5. Server Room and Secretariat Security Improvements	€ 1,500.00	€ 1,549.50	€ 1,600.63	€ 1,653.45	€ 6,832.07	**€ 13,135.66**
3.6. UPS	€ 0.00	€ 0.00	€ 0.00	€ 0.00	€ 0.00	**€ 0.00**
3.7 Workstations	€ 0.00	€ 4,132.00	€ 0.00	€ 4,409.21	€ 0.00	**€ 8,541.21**
4. Contingencies (@ 1.1%)	€ 895.64	€ 925.20	€ 955.73	€ 987.27	€ 1,076.21	**€ 4,840.06**
5. Annual Inflation Rate	**3.3%**	**3.3%**	**3.3%**	**3.3%**	**3.3%**	**-**
Annual Indicative OpEx	€ 82,317.77	€ 85,034.25	€ 87,840.38	€ 90,739.11	€ 98,913.93	**€ 444,845.44**

6. Conclusion

Based on the above, it can be concluded that either hosting option (or *delivery model*) for the SIOFA VMS would be able to provide a SIOFA VMS that adequately fulfils the functions required by CMM 16 (2023) while being compliant with other SIOFA CMMs and the SIOFA VMS SSPs. The MoP should, therefore, look at other factors to determine which hosting option it will choose for the SIOFA VMS.

In terms of cost and resource requirements, it is quite evident that SaaS applications offer a better value proposition than their SaaP counterpart, potentially saving the MoP up to EUR 350,000 in the first six years of its operation. While this may come with some compromises with respect to how secure SaaS applications may be and the level of control available to the end user, these limitations are not very significant, as there are other RFMOs with Secretariat of comparable size (such as NPFC and SPRFMO) that are already satisfactorily using SaaS for their VMS applications, also recalling that these risks may be mitigated or eliminated completely depending on the service provider.

A SaaS deployment should also be less demanding in terms of Secretariat staffing requirements.

Moreover, SaaP may not necessarily be as flexible as SaaS should the objective of the SIOFA VMS be broadened in the future, something that is not uncommon in other RFMOs. This includes implementing other tools within the SIOFA VMS, such as electronic reporting systems and automatic identification systems, which may further enhance SIOFA's capacity to fulfil its mandate and objectives under the Agreement.